https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Mar 2025 Vol. 12 No. 05

Table of Content

Vendor	Product	Page Number
Qualcomm	immersive_home_216_firmware	673
	immersive_home_316_firmware	673
	immersive_home_318_firmware	673
	immersive_home_3210_firmware	673
	immersive_home_326_firmware	674
	ipq5010_firmware	674
	ipq5028_firmware	674
	ipq5300_firmware	674
	ipq5302_firmware	674
	ipq5312_firmware	675
	ipq5332_firmware	675
	ipq6000_firmware	675
	ipq6010_firmware	675
	ipq6018_firmware	675
	ipq6028_firmware	676
	ipq8070a_firmware	676
	ipq8071a_firmware	676
	ipq8072a_firmware	676
	ipq8074a_firmware	676
	ipq8076a_firmware	677
	ipq8076_firmware	677
	ipq8078a_firmware	677
	ipq8078_firmware	677
	ipq8173_firmware	677
	ipq8174_firmware	678
	ipq9008_firmware	678
	ipq9048_firmware	678
	ipq9554_firmware	678
	ipq9570_firmware	678
	ipq9574_firmware	679
	mdm9205s_firmware	679
	mdm9628_firmware	679
	mdm9640_firmware	680

Vendor	Product	Page Number
Qualcomm	qcm5430_firmware	738
	qcm6125_firmware	739
	qcm6490_firmware	740
	qcm8550_firmware	741
	qcn5021_firmware	742
	qcn5022_firmware	742
	qcn5024_firmware	742
	qcn5052_firmware	743
	qcn5054_firmware	743
	qcn5122_firmware	743
	qcn5124_firmware	743
	qcn5152_firmware	743
	qcn5154_firmware	744
	qcn5164_firmware	744
	qcn6023_firmware	744
	qcn6024_firmware	744
	qcn6100_firmware	745
	qcn6102_firmware	745
	qcn6112_firmware	746
	qcn6122_firmware	746
	qcn6132_firmware	746
	qcn6224_firmware	746
	qcn6274_firmware	747
	qcn6402_firmware	749
	qcn6412_firmware	749
	qcn6422_firmware	749
	qcn6432_firmware	749
	qcn7606_firmware	750
	qcn9000_firmware	750
	qcn9011_firmware	750
	qcn9012_firmware	751
	qcn9022_firmware	751
	qcn9024_firmware	752

Vendor	Product	Page Number
Qualcomm	snapdragon_870_5g_firmware	879
	snapdragon_888\+_5g_firmware	880
	snapdragon_888_5g_firmware	881
	snapdragon_8cx_gen_3_compute_firmware	882
	snapdragon_8\+_gen_1_firmware	882
	snapdragon_8\+_gen_2_firmware	883
	snapdragon_8\+_gen_2_mobile_firmware	884
	snapdragon_8_gen_1_firmware	884
	snapdragon_8_gen_2_firmware	886
	snapdragon_8_gen_2_mobile_firmware	887
	snapdragon_8_gen_3_firmware	887
	snapdragon_ar1_gen_1_firmware	888
	snapdragon_ar1_gen_1__firmware	889
	snapdragon_ar2_gen_1_firmware	889
	snapdragon_ar2_gen_1__firmware	890
	snapdragon_auto_4g_firmware	890
	snapdragon_auto_5g-rf_firmware	891
	snapdragon_auto_5g-rf_gen_2_firmware	891
	snapdragon_auto_5g_firmware	891
	snapdragon_auto_5g_modem-rf_firmware	891
	snapdragon_auto_5g_modem-rf_gen_2_firmware	892
	snapdragon_w5\+_gen_1_firmware	893
	snapdragon_w5\+_gen_1_wearable_firmware	893
	snapdragon_wear_1300_firmware	894
	snapdragon_wear_4100\+_firmware	894
	snapdragon_wear_4100\+__firmware	894
	snapdragon_x12_lte_firmware	895
	snapdragon_x24_lte_firmware	895
	snapdragon_x35_5g-rf_firmware	895
	snapdragon_x35_5g_firmware	895
	snapdragon_x50_5g_firmware	896

Vendor	Product	Page Number
Qualcomm	snapdragon_x55_5g-rf_firmware	897
	snapdragon_x55_5g_firmware	897
	snapdragon_x5_lte_firmware	898
	snapdragon_x62_5g-rf_firmware	898
	snapdragon_x62_5g_firmware	899
	snapdragon_x65_5g-rf_firmware	899
	snapdragon_x65_5g_firmware	900
	snapdragon_x70-rf_firmware	901
	snapdragon_x72_5g-rf_firmware	901
	snapdragon_x72_5g_firmware	901
	snapdragon_x75_5g-rf_firmware	902
	snapdragon_x75_5g_firmware	902
	snapdragon_xr1_firmware	904
	snapdragon_xr2\+_gen_1_firmware	904
	snapdragon_xr2_5g_firmware	905
	snapdragon_xr2_5g__firmware	905
	srv1h_firmware	906
	srv1l_firmware	908
	srv1m_firmware	910
	ssg2115p_firmware	912
	ssg2125p_firmware	912
	sw5100p_firmware	913
	sw5100_firmware	914
	sxr1120_firmware	915
	sxr1230p_firmware	916
	sxr2130_firmware	916
	sxr2230p_firmware	917
	sxr2250p_firmware	919
	sxr2330p_firmware	921
	talynplus_firmware	922
	video_collaboration_vc1_firmware	923
	video_collaboration_vc3_firmware	924
	video_collaboration_vc5_firmware	925

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 18.0					
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	A-APP-SAFA-180325/1
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	A-APP-SAFA-180325/2
Affected Version(s): * Up to (excluding) 18.3.1					
Out-of-bounds Write	11-Mar-2025	8.8	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS	https://support.apple.com/en-us/122281, https://support.apple.com/en-us/122283,	A-APP-SAFA-180325/3

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). **CVE ID: CVE-2025-24201**	https://support.apple.com/en-us/122284, https://support.apple.com/en-us/122285	
Vendor: assimp					
Product: assimp					
Affected Version(s): 5.4.3					
Improper Restriction of Operations within the Bounds of a Memory Buffer	10-Mar-2025	6.3	A vulnerability, which was classified as critical, has been found in Open Asset Import Library Assimp 5.4.3. This issue affects the function Assimp::BaseImporter::ConvertToUTF8 of the file BaseImporter.cpp of the component File Handler. The manipulation leads to heap-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2152**	N/A	A-ASS-ASSI-180325/4
Vendor: auctionplugin					
Product: ultimate_auction					
Affected Version(s): * Up to (excluding) 4.3.0					
Improper Input Validation	04-Mar-2025	5.4	The Ultimate WordPress Auction Plugin plugin for WordPress is vulnerable to unauthorized access to functionality in all versions up to, and including, 4.2.9. This makes it possible for	https://plugins.trac.wordpress.org/changeset/3242416/ultimate-auction/trunk/u	A-AUC-ULTI-180325/5

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
			authenticated attackers, with Contributor-level access and above, to delete arbitrary auctions, posts as well as pages and allows them to execute other actions related to auction handling. **CVE ID: CVE-2025-0958**	ltimate-auction.php	
Vendor: axelkeller					
Product: gpx_viewer					
Affected Version(s): * Up to (including) 2.2.11					
Path Traversal: '.../...//'	03-Mar-2025	4.9	Path Traversal vulnerability in NotFound GPX Viewer allows Path Traversal. This issue affects GPX Viewer: from n/a through 2.2.11. **CVE ID: CVE-2025-27274**	N/A	A-AXE-GPX_-180325/6
Vendor: Bestwebsoft					
Product: smtp					
Affected Version(s): * Up to (excluding) 1.2.0					
Unrestricted Upload of File with Dangerous Type	08-Mar-2025	7.2	The SMTP by BestWebSoft plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'save_options' function in all versions up to, and including, 1.1.9. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-13908**	https://plugins.trac.wordpress.org/changeset/3250935/	A-BES-SMTP-180325/7
Vendor: binary-husky					
Product: gpt_academic					
Affected Version(s): *					
Improper Link	03-Mar-2025	7.5	GPT Academic provides interactive interfaces for	https://github.com/binary-	A-BIN-GPT_-180325/8

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
Resolution Before File Access ('Link Following')			large language models. In 3.91 and earlier, GPT Academic does not properly account for soft links. An attacker can create a malicious file as a soft link pointing to a target file, then package this soft link file into a tar.gz file and upload it. Subsequently, when accessing the decompressed file from the server, the soft link will point to the target file on the victim server. The vulnerability allows attackers to read all files on the server. **CVE ID: CVE-2025-25185**	husky/gpt_academic/commit/5dffe8627f681d7006cebcba27def038bb691949, https://github.com/binary-husky/gpt_academic/security/advisories/GHSA-gqp5-wm97-qxcv	
Vendor: changeweb					
Product: unifiedtransform					
Affected Version(s): 2.0					
N/A	10-Mar-2025	4.3	Unifiedtransform 2.0 is vulnerable to Incorrect Access Control, which allows students to modify rules for exams. The affected endpoint is /exams/edit-rule?exam_rule_id=1. **CVE ID: CVE-2025-25616**	N/A	A-CHA-UNIF-180325/9
N/A	10-Mar-2025	2.7	Unifiedtransform 2.0 is vulnerable to Incorrect Access Control which allows viewing attendance list for all class sections. **CVE ID: CVE-2025-25615**	N/A	A-CHA-UNIF-180325/10
Vendor: code-projects					
Product: blood_bank_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	04-Mar-2025	3.5	A vulnerability, which was classified as problematic, has been found in code-projects Blood Bank System 1.0. Affected by this issue is some unknown functionality of the file /Blood/A+.php.	N/A	A-COD-BLOO-180325/11

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
('Cross-site Scripting')			The manipulation of the argument Availibility leads to cross site scripting. The attack may be launched remotely. **CVE ID: CVE-2025-1904**		
Vendor: coderevolution					
Product: aiomatic					
Affected Version(s): * Up to (excluding) 2.3.9					
Unrestricted Upload of File with Dangerous Type	08-Mar-2025	8.8	The Aiomatic - Automatic AI Content Writer & Editor, GPT-3 & GPT-4, ChatGPT ChatBot & AI Toolkit plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'aiomatic_generate_featured_image' function in all versions up to, and including, 2.3.8. This makes it possible for authenticated attackers, with Contributor-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-13882**	N/A	A-COD-AIOM-180325/12
Vendor: codezips					
Product: online_shopping_website					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	7.3	A vulnerability was found in Codezips Online Shopping Website 1.0. It has been rated as critical. This issue affects some unknown processing of the file /cart_add.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	N/A	A-COD-ONLI-180325/13

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
			CVE ID: CVE-2025-1903		
Vendor: cozyvision					
Product: sms_alert_order_notifications					
Affected Version(s): * Up to (excluding) 3.7.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.3	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cozy Vision SMS Alert Order Notifications – WooCommerce allows SQL Injection. This issue affects SMS Alert Order Notifications – WooCommerce: from n/a through 3.7.8. **CVE ID: CVE-2025-26988**	N/A	A-COZ-SMS_-180325/14
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	7.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozy Vision SMS Alert Order Notifications – WooCommerce allows Reflected XSS. This issue affects SMS Alert Order Notifications – WooCommerce: from n/a through 3.7.8. **CVE ID: CVE-2025-26984**	N/A	A-COZ-SMS_-180325/15
Vendor: crowdytheme					
Product: arolax					
Affected Version(s): * Up to (excluding) 1.7					
Missing Authorization	04-Mar-2025	8.8	The Animation Addons for Elementor Pro plugin for WordPress is vulnerable to unauthorized arbitrary plugin installation due to a missing capability check on the install_elementor_plugin_handler() function in all versions up to, and including, 1.6. This makes it possible for authenticated	N/A	A-CRO-AROL-180325/16

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
			attackers, with Subscriber-level access and above, to install and activate arbitrary plugins which can be leveraged to further infect a victim when Elementor is not activated on a vulnerable site. **CVE ID: CVE-2025-1639**		
Vendor: danielgatis					
Product: rembg					
Affected Version(s): * Up to (including) 2.0.57					
Server-Side Request Forgery (SSRF)	03-Mar-2025	7.5	Rembg is a tool to remove images background. In Rembg 2.0.57 and earlier, the /api/remove endpoint takes a URL query parameter that allows an image to be fetched, processed and returned. An attacker may be able to query this endpoint to view pictures hosted on the internal network of the rembg server. This issue may lead to Information Disclosure. **CVE ID: CVE-2025-25301**	N/A	A-DAN-REMB-180325/17
Vendor: dasinfomedia					
Product: school_management_system					
Affected Version(s): * Up to (including) 93.0.0					
Authentication Bypass Using an Alternate Path or Channel	07-Mar-2025	8.8	The School Management System for Wordpress plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 93.0.0. This is due to the plugin not properly validating a user's identity prior to updating their details like email and password through the mj_smgt_update_user() and mj_smgt_add_admission() functions, along with a local	N/A	A-DAS-SCHO-180325/18

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			file inclusion vulnerability. This makes it possible for authenticated attackers, with student-level access and above, to change arbitrary user's email addresses and passwords, including administrators, and leverage that to gain access to their account. This was escalated four months ago after no response to our initial outreach, yet it still vulnerable. **CVE ID: CVE-2024-9658**		
Vendor: Ddsn					
Product: acora_cms					
Affected Version(s): 10.1.1					
Cross-Site Request Forgery (CSRF)	03-Mar-2025	8.8	Acora CMS version 10.1.1 is vulnerable to Cross-Site Request Forgery (CSRF). This flaw enables attackers to trick authenticated users into performing unauthorized actions, such as account deletion or user creation, by embedding malicious requests in external content. The lack of CSRF protections allows exploitation via crafted requests. **CVE ID: CVE-2025-25967**	N/A	A-DDS-ACOR-180325/19
Vendor: dpgaspar					
Product: flask-appbuilder					
Affected Version(s): * Up to (excluding) 4.5.3					
Observable Response Discrepancy	03-Mar-2025	3.7	Flask-AppBuilder is an application development framework. Prior to 4.5.3, Flask-AppBuilder allows unauthenticated users to enumerate existing usernames by timing the response time from the server when brute forcing	https://github.com/dpgaspar/Flask-AppBuilder/security/advisories/GHSA-p8q5-cvwx-wvwp	A-DPG-FLAS-180325/20

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			requests to login. This vulnerability is fixed in 4.5.3. **CVE ID: CVE-2025-24023**		
Vendor: e4jconnect					
Product: vikrentcar					
Affected Version(s): * Up to (excluding) 1.4.3					
Cross-Site Request Forgery (CSRF)	08-Mar-2025	8.8	The VikRentCar Car Rental Management System plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.2. This is due to missing or incorrect nonce validation on the 'save' function. This makes it possible for unauthenticated attackers to change plugin access privileges via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Successful exploitation allows attackers with subscriber-level privileges and above to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2024-11640**	https://plugins.trac.wordpress.org/changeset/3225040/vikrentcar	A-E4J-VIKR-180325/21
Vendor: easyvirt					
Product: dc_netscope					
Affected Version(s): * Up to (including) 8.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	5.4	Multiple cross-site scripting (XSS) vulnerabilities in EasyVirt DC NetScope <= 8.6.4 allow remote attackers to inject arbitrary JavaScript or HTML code via the (1) smtp_server, (2) smtp_account, (3) smtp_password, or (4) email_recipients parameter to /smtp/update; the (5) ntp	N/A	A-EAS-DC_N-180325/22

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or (6) dns parameter to /proxy/ntp/change; the (7) newVcenterAddress parameter to /process_new_vcenter. **CVE ID: CVE-2024-55064**		
Vendor: Esri					
Product: arcgis_server					
Affected Version(s): From (including) 10.9.1 Up to (including) 11.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	8.7	A SQL injection vulnerability in ArcGIS Server allows an EDIT operation to modify Column properties allowing for the execution of a SQL Injection by a remote authenticated user with elevated (non admin) privileges. There is a high impact to integrity and confidentiality and no impact to availability. **CVE ID: CVE-2024-51962**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/23
Improper Access Control	03-Mar-2025	8.5	There is an improper access control issue in ArcGIS Server versions 10.9.1 through 11.3 on Windows and Linux, which under unique circumstances, could potentially allow a remote, low privileged authenticated attacker to access secure services published a standalone (Unfederated) ArcGIS Server instance. If successful this compromise would have a high impact on Confidentiality, low impact on integrity and no impact to availability of the software. **CVE ID: CVE-2024-51954**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/24
External Control of File Name or Path	03-Mar-2025	7.5	There is a local file inclusion vulnerability in ArcGIS Server 10.9.1 thru 11.3 that may allow a remote,	https://www.esri.com/arcgis-blog/products/trust-	A-ESR-ARCG-180325/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to craft a URL that could potentially disclose sensitive configuration information by reading internal files from the remote server. Due to the nature of the files accessible in this vulnerability the impact to confidentiality is High there is no impact to both integrity or availability. **CVE ID: CVE-2024-51961**	arcgis/administration/arcgis-server-security-2025-update-1-patch/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Mar-2025	4.9	There is a path traversal vulnerability in ESRI ArcGIS Server versions 10.9.1 thru 11.3. Successful exploitation may allow a remote authenticated attacker with admin privileges to traverse the file system to access files outside of the intended directory. There is no impact to integrity or availability due to the nature of the files that can be accessed, but there is a potential high impact to confidentiality. **CVE ID: CVE-2024-51966**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/26
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Mar-2025	4.9	There is a path traversal vulnerability in ESRI ArcGIS Server versions 10.9.1 thru 11.3. Successful exploitation may allow a remote authenticated attacker with admin privileges to traverse the file system to access files outside of the intended directory. There is no impact to integrity or availability due to the nature of the files that can be accessed, but there is a potential high impact to confidentiality.	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/27

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-51958		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51960**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/28
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51959**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/29
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/30

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51951**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51957**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/31
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51956**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/32
Improper Neutralization of Input During Web Page	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated	https://www.esri.com/arcgis-blog/products/trust-arcgis/administ	A-ESR-ARCG-180325/33

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51953**	ration/arcgis-server-security-2025-update-1-patch/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51952**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/34
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability.	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/35

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-51950		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51949**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/36
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51948**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/37
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/38

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51947**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51946**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/39
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51945**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/40
Improper Neutralization of Input During Web Page	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated	https://www.esri.com/arcgis-blog/products/trust-arcgis/administ	A-ESR-ARCG-180325/41

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51944**	ration/arcgis-server-security-2025-update-1-patch/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51942**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/42
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability.	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/43

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
			CVE ID: CVE-2024-10904		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-51963**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	4.8	There is a stored Cross-site Scripting vulnerability in ArcGIS Server for versions 10.9.1 – 11.3 that may allow a remote, authenticated attacker to create a stored crafted link which when clicked could potentially execute arbitrary JavaScript code in the victim's browser. The privileges required to execute this attack are high, requiring publisher capabilities. The impact is low to both confidentiality and integrity while having no impact to availability. **CVE ID: CVE-2024-5888**	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	A-ESR-ARCG-180325/45
Vendor: F5					
Product: nginx					
Affected Version(s): From (including) 1.29.1 Up to (excluding) 1.34.2					
Loop with Unreachable Exit Condition ('Infinite Loop')	04-Mar-2025	5.3	In NGINX Unit before version 1.34.2 with the Java Language Module in use, undisclosed requests can lead to an infinite loop and cause an increase in CPU	https://my.f5.com/manage/s/article/K000149959	A-F5-NGIN-180325/46

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
			resource utilization. This vulnerability allows a remote attacker to cause a degradation that can lead to a limited denial-of-service (DoS). There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated. **CVE ID: CVE-2025-1695**		
Vendor: fancywp					
Product: starter_templates					
Affected Version(s): * Up to (including) 2.0.0					
Server-Side Request Forgery (SSRF)	08-Mar-2025	5.3	The Starter Templates by FancyWP plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 2.0.0 via the 'http_request_host_is_external' filter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. **CVE ID: CVE-2024-13924**	N/A	A-FAN-STAR-180325/47
Vendor: fooplugins					
Product: foogallery					
Affected Version(s): * Up to (excluding) 2.4.30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2025	6.4	The FooGallery – Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the default_gallery_title_size parameter in all versions up	N/A	A-FOO-FOOG-180325/48

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
			to, and including, 2.4.29 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with granted gallery and album creator roles, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-12119**		
Authorization Bypass Through User-Controlled Key	08-Mar-2025	4.3	The FooGallery – Responsive Photo Gallery, Image Viewer, Justified, Masonry & Carousel plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.4.29 via the foogallery_attachment_modal_save AJAX action due to missing validation on a user controlled key (img_id). This makes it possible for authenticated attackers, with granted access and above, to update arbitrary post and page content. This requires the Gallery Creator Role setting to be a value lower than 'Editor' for there to be any real impact. **CVE ID: CVE-2024-12114**	https://plugins.trac.wordpress.org/changeset/3250684/foogallery/tags/2.4.30/includes/admin/class-gallery-attachment-modal.php?old=3229839&old_path=foogallery%2Ftags%2F2.4.29%2Fincludes%2Fadmin%2Fclass-gallery-attachment-modal.php	A-FOO-FOOG-180325/49
Vendor: ftcms					
Product: ftcms					
Affected Version(s): 2.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Mar-2025	4.7	A vulnerability classified as critical has been found in ftcms 2.1. Affected is an unknown function of the file /admin/index.php/web/ajax_all_lists of the component Search. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely.	N/A	A-FTC-FTCM-180325/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-2132**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Mar-2025	2.4	A vulnerability classified as problematic was found in ftcms 2.1. Affected by this vulnerability is an unknown functionality of the file /admin/index.php/news/edit. The manipulation of the argument title leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-2133**	N/A	A-FTC-FTCM-180325/51
Vendor: funnelkit					
Product: slingblocks					
Affected Version(s): * Up to (excluding) 1.6.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2025	6.4	The SlingBlocks – Gutenberg Blocks by FunnelKit (Formerly WooFunnels) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the "Icon List" Block in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3251693%40slingblocks&new=3251693%40slingblocks&sfp_email=&sfph_mail=#file5	A-FUN-SLIN-180325/52

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
			CVE ID: CVE-2024-13675		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): 17.9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	8.7	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1. A proxy feature could potentially allow unintended content rendering leading to XSS under specific circumstances. **CVE ID: CVE-2025-0475**	N/A	A-GIT-GITL-180325/53
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	7.7	A Cross Site Scripting (XSS) vulnerability in GitLab-EE affecting all versions from 16.6 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1 allows an attacker to bypass security controls and execute arbitrary scripts in a users browser under specific conditions. **CVE ID: CVE-2025-0555**	N/A	A-GIT-GITL-180325/54
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	5.4	An issue has been discovered in GitLab CE/EE affecting all versions from 16.6 before 17.7.6, 17.8 before 17.8.4, and 17.9 before 17.9.1. An attacker could inject HMTL into the child item search potentially leading to XSS in certain situations. **CVE ID: CVE-2024-8186**	N/A	A-GIT-GITL-180325/55
Affected Version(s): From (including) 15.10.0 Up to (excluding) 17.7.6					
Improper Neutralization of Input During Web Page	03-Mar-2025	8.7	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9	N/A	A-GIT-GITL-180325/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			prior to 17.9.1. A proxy feature could potentially allow unintended content rendering leading to XSS under specific circumstances. **CVE ID: CVE-2025-0475**		
Affected Version(s): From (including) 16.6.0 Up to (excluding) 17.7.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	7.7	A Cross Site Scripting (XSS) vulnerability in GitLab-EE affecting all versions from 16.6 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1 allows an attacker to bypass security controls and execute arbitrary scripts in a users browser under specific conditions. **CVE ID: CVE-2025-0555**	N/A	A-GIT-GITL-180325/57
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	5.4	An issue has been discovered in GitLab CE/EE affecting all versions from 16.6 before 17.7.6, 17.8 before 17.8.4, and 17.9 before 17.9.1. An attacker could inject HMTL into the child item search potentially leading to XSS in certain situations. **CVE ID: CVE-2024-8186**	N/A	A-GIT-GITL-180325/58
Affected Version(s): From (including) 17.8.0 Up to (excluding) 17.8.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	8.7	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1. A proxy feature could potentially allow unintended content rendering leading to XSS under specific circumstances. **CVE ID: CVE-2025-0475**	N/A	A-GIT-GITL-180325/59
Improper Neutralizati	03-Mar-2025	7.7	A Cross Site Scripting (XSS) vulnerability in GitLab-EE	N/A	A-GIT-GITL-180325/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			affecting all versions from 16.6 prior to 17.7.6, 17.8 prior to 17.8.4, and 17.9 prior to 17.9.1 allows an attacker to bypass security controls and execute arbitrary scripts in a users browser under specific conditions. **CVE ID: CVE-2025-0555**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	5.4	An issue has been discovered in GitLab CE/EE affecting all versions from 16.6 before 17.7.6, 17.8 before 17.8.4, and 17.9 before 17.9.1. An attacker could inject HMTL into the child item search potentially leading to XSS in certain situations. **CVE ID: CVE-2024-8186**	N/A	A-GIT-GITL-180325/61
Vendor: givewp					
Product: givewp					
Affected Version(s): * Up to (excluding) 3.20.0					
Deserialization of Untrusted Data	04-Mar-2025	9.8	The Donations Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.19.4 via deserialization of untrusted input from the Donation Form through the 'card_address' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to achieve remote code execution. **CVE ID: CVE-2025-0912**	https://github.com/impress-org/givewp/pull/7679/files, https://plugins.trac.wordpress.org/changeset/3234114/give/trunk/src/Donations/Properties/BillingAddress.php	A-GIV-GIVE-180325/62
Vendor: GNU					
Product: grub2					
Affected Version(s): * Up to (including) 2.12					

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	6.7	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based out-of-bounds writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass. **CVE ID: CVE-2024-45782**	N/A	A-GNU-GRUB-180325/63
Out-of-bounds Write	03-Mar-2025	6.7	A flaw was found in grub2. When reading tar files, grub2 allocates an internal buffer for the file name. However, it fails to properly verify the allocation against possible integer overflows. It's possible to cause the allocation length to overflow with a crafted tar file, leading to a heap out-of-bounds write. This flaw eventually allows an attacker to circumvent secure boot protections. **CVE ID: CVE-2024-45780**	N/A	A-GNU-GRUB-180325/64
Out-of-bounds Write	03-Mar-2025	6.4	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a	N/A	A-GNU-GRUB-180325/65

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections. **CVE ID: CVE-2025-0678**		
Integer Overflow or Wraparound	03-Mar-2025	4.1	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash. **CVE ID: CVE-2024-45778**	N/A	A-GNU-GRUB-180325/66
Out-of-bounds Read	03-Mar-2025	4.1	An integer overflow flaw was found in the BFS file system driver in grub2. When reading a file with an indirect extent map, grub2 fails to validate the number of extent entries to be read. A crafted or corrupted BFS filesystem may cause an integer overflow during the file reading, leading to a heap of bounds read. As a consequence, sensitive data may be leaked, or grub2 will crash. **CVE ID: CVE-2024-45779**	N/A	A-GNU-GRUB-180325/67
Vendor: Hdfgroup					
Product: hdf5					
Affected Version(s): 1.14.6					
Improper Restriction of Operations within the Bounds of a	10-Mar-2025	5	A vulnerability, which was classified as critical, was found in HDF5 1.14.6. Affected is the function H5SM_delete of the file H5SM.c of the component h5 File Handler. The	N/A	A-HDF-HDF5-180325/68

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
Memory Buffer			manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2153**		
Vendor: heroplugins					
Product: hero_maps_premium					
Affected Version(s): * Up to (including) 2.3.9					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Mar-2025	6.5	The Hero Maps Premium plugin for WordPress is vulnerable to SQL Injection via several AJAX actions in all versions up to, and including, 2.3.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-13781**	N/A	A-HER-HERO-180325/69
Vendor: IBM					
Product: aspera_shares					
Affected Version(s): 1.10.0					
Improper Restriction of XML External Entity Reference	07-Mar-2025	7.1	IBM Aspera Shares 1.9.9 through 1.10.0 PL7 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to expose	https://www.ibm.com/support/pages/node/7185096	A-IBM-ASPE-180325/70

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive information or consume memory resources. **CVE ID: CVE-2025-0162**		
Affected Version(s): From (including) 1.9.9 Up to (excluding) 1.10.0					
Improper Restriction of XML External Entity Reference	07-Mar-2025	7.1	IBM Aspera Shares 1.9.9 through 1.10.0 PL7 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to expose sensitive information or consume memory resources. **CVE ID: CVE-2025-0162**	https://www.ibm.com/support/pages/node/7185096	A-IBM-ASPE-180325/71
Product: engineering_requirements_management_doors_next					
Affected Version(s): 7.0.2					
Download of Code Without Integrity Check	03-Mar-2025	8.8	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a user to download a malicious file without verifying the integrity of the code. **CVE ID: CVE-2024-43169**	https://www.ibm.com/support/pages/node/7184506	A-IBM-ENGI-180325/72
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information. **CVE ID: CVE-2024-41771**	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/73
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information.	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-41770		
Affected Version(s): 7.0.3					
Download of Code Without Integrity Check	03-Mar-2025	8.8	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a user to download a malicious file without verifying the integrity of the code. **CVE ID: CVE-2024-43169**	https://www.ibm.com/support/pages/node/7184506	A-IBM-ENGI-180325/75
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information. **CVE ID: CVE-2024-41770**	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/76
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information. **CVE ID: CVE-2024-41771**	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/77
Affected Version(s): 7.1					
Download of Code Without Integrity Check	03-Mar-2025	8.8	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a user to download a malicious file without verifying the integrity of the code. **CVE ID: CVE-2024-43169**	https://www.ibm.com/support/pages/node/7184506	A-IBM-ENGI-180325/78
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information.	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/79

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-41771		
Insufficiently Protected Credentials	03-Mar-2025	7.5	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information. **CVE ID: CVE-2024-41770**	https://www.ibm.com/support/pages/node/7184663	A-IBM-ENGI-180325/80
Product: sterling_control_center					
Affected Version(s): 6.2.1					
Improper Neutralization of HTTP Headers for Scripting Syntax	07-Mar-2025	5.4	IBM Control Center 6.2.1 through 6.3.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. **CVE ID: CVE-2023-35894**	https://www.ibm.com/support/pages/node/7185101	A-IBM-STER-180325/81
Affected Version(s): 6.3.1					
Improper Neutralization of HTTP Headers for Scripting Syntax	07-Mar-2025	5.4	IBM Control Center 6.2.1 through 6.3.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. **CVE ID: CVE-2023-35894**	https://www.ibm.com/support/pages/node/7185101	A-IBM-STER-180325/82
Vendor: imithemes					
Product: eventer					
Affected Version(s): * Up to (excluding) 3.9.9.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Injection: Hibernate	07-Mar-2025	8.8	The Eventer - WordPress Event & Booking Manager Plugin plugin for WordPress is vulnerable to SQL Injection via the reg_id parameter in all versions up to, and including, 3.9.9.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2025-0959**	N/A	A-IMI-EVEN-180325/83
Vendor: javothemes					
Product: javo_core					
Affected Version(s): * Up to (excluding) 3.0.0.266					
Improper Privilege Management	08-Mar-2025	9.8	The Javo Core plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 3.0.0.080. This is due to the plugin allowing users who are registering new accounts to set their own role. This makes it possible for unauthenticated attackers to gain elevated privileges by creating an account with the administrator role. **CVE ID: CVE-2025-0177**	N/A	A-JAV-JAVO-180325/84
Vendor: joomlaux					
Product: jux_real_estate					
Affected Version(s): 3.4.0					
Improper Neutralizati on of Special	09-Mar-2025	6.3	A vulnerability was found in JoomlaUX JUX Real Estate 3.4.0 on Joomla and	N/A	A-JOO-JUX_-180325/85

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
Elements in Output Used by a Downstream Component ('Injection')			classified as critical. This issue affects some unknown processing of the file /extensions/realestate/index.php/properties/list/list-with-sidebar/realties of the component GET Parameter Handler. The manipulation of the argument title leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-2126**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2025	4.3	A vulnerability was found in JoomlaUX JUX Real Estate 3.4.0 on Joomla. It has been classified as problematic. Affected is an unknown function of the file /extensions/realestate/index.php/properties/list/list-with-sidebar/realties. The manipulation of the argument Itemid/jp_yearbuilt leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-2127**	N/A	A-JOO-JUX_-180325/86
Vendor: jozoor					
Product: shortcode_cleaner_lite					
Affected Version(s): * Up to (including) 1.0.9					
Missing Authorization	08-Mar-2025	6.5	The Shortcode Cleaner Lite plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the download_backup()	N/A	A-JOZ-SHOR-180325/87

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function in all versions up to, and including, 1.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export arbitrary options. **CVE ID: CVE-2025-1481**		
Vendor: jtsternberg					
Product: code_snippets_cpt					
Affected Version(s): * Up to (including) 2.1.0					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2025	4.3	The The Code Snippets CPT plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.1.0. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes. **CVE ID: CVE-2024-13895**	N/A	A-JTS-CODE-180325/88
Vendor: master-addons					
Product: master_addons					
Affected Version(s): * Up to (excluding) 2.0.7.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	6.4	The Master Addons – Elementor Addons with White Label, Free Widgets, Hover Effects, Conditions, & Animations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 2.0.7.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-	https://plugins.trac.wordpress.org/changeset/3243199/	A-MAS-MAST-180325/89

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
			level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2025-0433**		
Affected Version(s): * Up to (excluding) 2.0.7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	6.4	The Master Addons – Elementor Addons with White Label, Free Widgets, Hover Effects, Conditions, & Animations plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple widgets in all versions up to, and including, 2.0.7.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-9618**	https://plugins.trac.wordpress.org/changeset/3243199/, https://plugins.trac.wordpress.org/changeset/3249130/	A-MAS-MAST-180325/90
Vendor: mayurik					
Product: best_online_news_portal					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "pagedescription" parameter in admin/aboutus.php. **CVE ID: CVE-2025-1870**	N/A	A-MAY-BEST-180325/91
Improper Neutralization of Special Elements used in an SQL	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "searchtitle" parameter in search.php.	N/A	A-MAY-BEST-180325/92

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID: CVE-2025-1875**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "description" parameter in admin/add-category.php. **CVE ID: CVE-2025-1874**	N/A	A-MAY-BEST-180325/93
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "pagetitle" and "pagedescription" parameters in admin/contactus.php. **CVE ID: CVE-2025-1873**	N/A	A-MAY-BEST-180325/94
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "sadminusername" parameter in admin/add-subadmins.php. **CVE ID: CVE-2025-1872**	N/A	A-MAY-BEST-180325/95
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "category" and "subcategory" parameters in admin/add-subcategory.php. **CVE ID: CVE-2025-1871**	N/A	A-MAY-BEST-180325/96
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Mar-2025	9.8	SQL injection vulnerability have been found in 101news affecting version 1.0 through the "username" parameter in admin/check_avalability.php. **CVE ID: CVE-2025-1869**	N/A	A-MAY-BEST-180325/97
Vendor: Microsoft					
Product: edge_chromium					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 134.0.3124.51					
The UI Performs the Wrong Action	07-Mar-2025	5.4	The UI performs the wrong action in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network. **CVE ID: CVE-2025-26643**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26643	A-MIC-EDGE-180325/98
Vendor: miniorange					
Product: social_login					
Affected Version(s): * Up to (including) 200.3.9					
Improper Authentication	08-Mar-2025	8.1	The miniOrange Social Login and Register (Discord, Google, Twitter, LinkedIn) Pro Addon plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 200.3.9. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username and the user does not have an already-existing account for the service returning the token. **CVE ID: CVE-2024-11087**	N/A	A-MIN-SOCI-180325/99
Vendor: mmaitre314					
Product: picklescan					
Affected Version(s): * Up to (excluding) 0.0.22					
Reliance on File Name or Extension of Externally-Supplied File	03-Mar-2025	9.8	picklescan before 0.0.22 only considers standard pickle file extensions in the scope for its vulnerability scan. An attacker could craft a malicious model that uses Pickle and include a malicious pickle file with a	N/A	A-MMA-PICK-180325/100

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			non-standard file extension. Because the malicious pickle file inclusion is not considered as part of the scope of picklescan, the file would pass security checks and appear to be safe, when it could instead prove to be problematic. **CVE ID: CVE-2025-1889**		
Vendor: mtrv					
Product: teachpress					
Affected Version(s): * Up to (excluding) 9.0.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	04-Mar-2025	6.5	The teachPress plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the 'tpsearch' shortcode in all versions up to, and including, 9.0.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2025-1321**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3246754%40teachpress&new=3246754%40teachpress&sfp_email=&sfph_mail=#file6	A-MTR-TEAC-180325/101
Vendor: nsquared					
Product: appointment_booking_calendar					
Affected Version(s): * Up to (excluding) 1.6.8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2025	6.1	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the accent_color and background parameter in all versions up to, and	https://plugins.trac.wordpress.org/changeset/3246760/simply-schedule-appointments/trunk/booking-app-	A-NSQ-APPO-180325/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			including, 1.6.8.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID: CVE-2024-13431**	new/iframe-inner.php	
Vendor: open5gs					
Product: open5gs					
Affected Version(s): * Up to (including) 2.7.2					
Improper Resource Shutdown or Release	04-Mar-2025	4.3	A vulnerability was found in Open5GS up to 2.7.2. It has been declared as problematic. Affected by this vulnerability is the function gmm_state_authentication of the file src/amf/gmm-sm.c of the component AMF. The manipulation leads to denial of service. The attack can be launched remotely. This vulnerability allows a single UE to crash the AMF, resulting in the complete loss of mobility and session management services and causing a network-wide outage. All registered UEs will lose connectivity, and new registrations will be blocked until the AMF is restarted, leading to a high availability impact. The exploit has been disclosed to the public and may be used. The patch is named e31e9965f00d9c744a7f728497cb4f3e97744ee8. It is recommended to apply a patch to fix this issue. **CVE ID: CVE-2025-1893**	https://github.com/open5gs/open5gs/commit/e31e9965f00d9c744a7f728497cb4f3e97744ee8	A-OPE-OPEN-180325/103

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: openxe					
Product: openxe					
Affected Version(s): * Up to (including) 1.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2025	3.5	A vulnerability was found in OpenXE up to 1.12. It has been declared as problematic. This vulnerability affects unknown code of the component Ticket Bearbeiten Page. The manipulation of the argument Notizen leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID: CVE-2025-2130**	N/A	A-OPE-OPEN-180325/104
Vendor: openziti					
Product: openziti					
Affected Version(s): * Up to (excluding) 3.7.1					
Server-Side Request Forgery (SSRF)	03-Mar-2025	8.6	OpenZiti is a free and open source project focused on bringing zero trust to any application. An endpoint on the admin panel can be accessed without any form of authentication. This endpoint accepts a user-supplied URL parameter to connect to an OpenZiti Controller and performs a server-side request, resulting in a potential Server-Side Request Forgery (SSRF) vulnerability. The fixed version has moved the request to the external controller from the server side to the client side, thereby eliminating the identity of the node from	N/A	A-OPE-OPEN-180325/105

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			being used to gain any additional permissions. This vulnerability is fixed in 3.7.1. **CVE ID: CVE-2025-27501**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	8.2	OpenZiti is a free and open source project focused on bringing zero trust to any application. An endpoint(/api/upload) on the admin panel can be accessed without any form of authentication. This endpoint accepts an HTTP POST to upload a file which is then stored on the node and is available via URL. This can lead to a stored cross site scripting attack if the file uploaded contains malicious code and is then accessed and executed within the context of the user's browser. This function is no longer necessary as the ziti-console moves from a node server application to a single page application, and has been disabled. The vulnerability is fixed in 3.7.1. **CVE ID: CVE-2025-27500**	N/A	A-OPE-OPEN-180325/106
Vendor: oxidized_web_project					
Product: oxidized_web					
Affected Version(s): * Up to (excluding) 0.15.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Mar-2025	9	In oxidized-web (aka Oxidized Web) before 0.15.0, the RANCID migration page allows an unauthenticated user to gain control over the Linux user account that is running oxidized-web. **CVE ID: CVE-2025-27590**	https://github.com/ytti/oxidized-web/commit/a5220a0ddc57b85cd122bffee228d3ed4901668e	A-OXI-OXID-180325/107
Vendor: phpgurukul					
Product: human_metapneumovirus					
Affected Version(s): 1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2025	3.5	A vulnerability was found in PHPGurukul Human Metapneumovirus Testing Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /search-report.php of the component Search Report Page. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2084**	N/A	A-PHP-HUMA-180325/108
Product: pre-school_enrollment_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Mar-2025	7.3	A vulnerability, which was classified as critical, was found in PHPGurukul Pre-School Enrollment System up to 1.0. Affected is an unknown function of the file /admin/profile.php. The manipulation of the argument fullname/emailid/mobileNumber leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2088**	N/A	A-PHP-PRE--180325/109
Product: restaurant_table_booking_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	7.3	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /add-table.php. The manipulation of the argument tableno leads to sql injection. The attack may be launched remotely. The	N/A	A-PHP-REST-180325/110

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
			exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1900**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	7.3	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/check_availability.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1901**	N/A	A-PHP-REST-180325/111
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	7.3	A vulnerability was found in PHPGurukul Restaurant Table Booking System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /search-result.php. The manipulation of the argument searchdata leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1894**	N/A	A-PHP-REST-180325/112
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	4.7	A vulnerability has been found in PHPGurukul Restaurant Table Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/profile.php. The manipulation of the argument mobilenumber leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other	N/A	A-PHP-REST-180325/113

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameters might be affected as well. **CVE ID: CVE-2025-1906**		
Product: student_record_system					
Affected Version(s): 3.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Mar-2025	7.3	A vulnerability was found in PHPGurukul Student Record System 3.2. It has been declared as critical. This vulnerability affects unknown code of the file /password-recovery.php. The manipulation of the argument emailid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1902**	N/A	A-PHP-STUD-180325/114
Vendor: platformly					
Product: platform.ly_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.1.7					
Server-Side Request Forgery (SSRF)	07-Mar-2025	5.3	The Platform.ly for WooCommerce plugin for WordPress is vulnerable to Blind Server-Side Request Forgery in all versions up to, and including, 1.1.6 via the 'hooks' function. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. **CVE ID: CVE-2024-13904**	https://plugins.trac.wordpress.org/changeset/3249460	A-PLA-PLAT-180325/115
Vendor: plechevandrey					
Product: wp-recall					
Affected Version(s): * Up to (excluding) 16.26.12					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2025	7.5	The WP-Recall – Registration, Profile, Commerce & More plugin for WordPress is vulnerable to SQL Injection via the 'databeat' parameter in all versions up to, and including, 16.26.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2025-1323**	https://plugins.trac.wordpress.org/changeset/3250094/wp-recall/trunk/add-on/rcl-chat/core.php	A-PLE-WP-R-180325/116
Exposure of Sensitive Information to an Unauthorized Actor	08-Mar-2025	4.3	The WP-Recall – Registration, Profile, Commerce & More plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 16.26.10 via the 'feed' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to view data from password protected, private, or draft posts that they should not have access to. **CVE ID: CVE-2025-1322**	https://plugins.trac.wordpress.org/changeset/3250094/wp-recall/trunk/add-on/rcl-chat/core.php	A-PLE-WP-R-180325/117
Vendor: prolizyazilim					
Product: student_affairs_information_system					
Affected Version(s): * Up to (excluding) 24.0927					
Improper Limitation of a Pathname to a Restricted Directory	03-Mar-2025	6.2	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Proliz Software OBS allows Path	N/A	A-PRO-STUD-180325/118

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			Traversal.This issue affects OBS: before 24.0927. **CVE ID: CVE-2024-8262**		
Authorization Bypass Through User-Controlled Key	03-Mar-2025	5.9	Authorization Bypass Through User-Controlled Key vulnerability in Proliz Software OBS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects OBS: before 24.0927. **CVE ID: CVE-2024-8261**	N/A	A-PRO-STUD-180325/119
Vendor: qzw1210					
Product: shishuocms					
Affected Version(s): 1.1					
Cross-Site Request Forgery (CSRF)	04-Mar-2025	4.3	A vulnerability was found in shishuocms 1.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1891**	N/A	A-QZW-SHIS-180325/120
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	2.4	A vulnerability was found in shishuocms 1.1. It has been classified as problematic. Affected is an unknown function of the file /manage/folder/add.json of the component Directory Deletion Page. The manipulation of the argument folderName leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1892**	N/A	A-QZW-SHIS-180325/121
Vendor: Redhat					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: openshift_container_platform					
Affected Version(s): 4.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	6.7	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based out-of-bounds writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass. **CVE ID: CVE-2024-45782**	N/A	A-RED-OPEN-180325/122
Out-of-bounds Write	03-Mar-2025	6.4	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections. **CVE ID: CVE-2025-0678**	N/A	A-RED-OPEN-180325/123

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	03-Mar-2025	4.1	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash. **CVE ID: CVE-2024-45778**	N/A	A-RED-OPEN-180325/124
Vendor: remyandrade					
Product: employee_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	3.5	A vulnerability, which was classified as problematic, was found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file employee.php. The manipulation of the argument Full Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID: CVE-2025-1905**	N/A	A-REM-EMPL-180325/125
Vendor: reprisesoftware					
Product: license_manager					
Affected Version(s): 14.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	6.1	Reprise License Manager 14.2 is vulnerable to reflected cross-site scripting in /goform/activate_process via the akey parameter. **CVE ID: CVE-2025-25939**	N/A	A-REP-LICE-180325/126
Vendor: rometheme					
Product: romethemekit_for_elementor					
Affected Version(s): * Up to (excluding) 1.5.4					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	08-Mar-2025	4.3	The RomethemeKit For Elementor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_options and reset_widgets functions in all versions up to, and including, 1.5.3. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify plugin settings or reset plugin widgets to their default state (all enabled). NOTE: This vulnerability was partially fixed in version 1.5.3. **CVE ID: CVE-2024-10326**	https://plugins.trac.wordpress.org/changeset/3220079/rometheme-for-elementor, https://plugins.trac.wordpress.org/changeset/3231792/rometheme-for-elementor	A-ROM-ROME-180325/127
Vendor: Ruby-lang					
Product: cgi					
Affected Version(s): * Up to (excluding) 0.3.5.1					
Allocation of Resources Without Limits or Throttling	04-Mar-2025	5.8	In the CGI gem before 0.4.2 for Ruby, the CGI::Cookie.parse method in the CGI library contains a potential Denial of Service (DoS) vulnerability. The method does not impose any limit on the length of the raw cookie value it processes. This oversight can lead to excessive resource consumption when parsing extremely large cookies. **CVE ID: CVE-2025-27219**	N/A	A-RUB-CGI-180325/128
N/A	04-Mar-2025	4	In the CGI gem before 0.4.2 for Ruby, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the Util#escapeElement method. **CVE ID: CVE-2025-27220**	N/A	A-RUB-CGI-180325/129
Affected Version(s): 0.3.6					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	04-Mar-2025	5.8	In the CGI gem before 0.4.2 for Ruby, the CGI::Cookie.parse method in the CGI library contains a potential Denial of Service (DoS) vulnerability. The method does not impose any limit on the length of the raw cookie value it processes. This oversight can lead to excessive resource consumption when parsing extremely large cookies. **CVE ID: CVE-2025-27219**	N/A	A-RUB-CGI-180325/130
N/A	04-Mar-2025	4	In the CGI gem before 0.4.2 for Ruby, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the Util#escapeElement method. **CVE ID: CVE-2025-27220**	N/A	A-RUB-CGI-180325/131
Affected Version(s): From (including) 0.4.0 Up to (excluding) 0.4.2					
Allocation of Resources Without Limits or Throttling	04-Mar-2025	5.8	In the CGI gem before 0.4.2 for Ruby, the CGI::Cookie.parse method in the CGI library contains a potential Denial of Service (DoS) vulnerability. The method does not impose any limit on the length of the raw cookie value it processes. This oversight can lead to excessive resource consumption when parsing extremely large cookies. **CVE ID: CVE-2025-27219**	N/A	A-RUB-CGI-180325/132
N/A	04-Mar-2025	4	In the CGI gem before 0.4.2 for Ruby, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the Util#escapeElement method. **CVE ID: CVE-2025-27220**	N/A	A-RUB-CGI-180325/133
Product: Ruby					
Affected Version(s): 3.1.0					

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
N/A	04-Mar-2025	4	In the CGI gem before 0.4.2 for Ruby, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the Util#escapeElement method. **CVE ID: CVE-2025-27220**	N/A	A-RUB-RUBY-180325/134
Affected Version(s): 3.2.0					
N/A	04-Mar-2025	4	In the CGI gem before 0.4.2 for Ruby, a Regular Expression Denial of Service (ReDoS) vulnerability exists in the Util#escapeElement method. **CVE ID: CVE-2025-27220**	N/A	A-RUB-RUBY-180325/135
Vendor: sfwebservice					
Product: injob					
Affected Version(s): * Up to (including) 3.5.1					
Authentication Bypass Using an Alternate Path or Channel	07-Mar-2025	9.8	The InWave Jobs plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 3.5.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account. **CVE ID: CVE-2025-1315**	N/A	A-SFW-INJO-180325/136
Vendor: shishuocms_project					
Product: shishuocms					
Affected Version(s): 1.1					
Improper Access Control	04-Mar-2025	6.3	A vulnerability has been found in shishuocms 1.1 and classified as critical. This vulnerability affects the function handleRequest of	N/A	A-SHI-SHIS-180325/137

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 file src/main/java/com/shishuo/cms/action/manage/ManageUpLoadAction.java. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1890**		
Vendor: sksdev					
Product: allow_php_execute					
Affected Version(s): 1.0					
Improper Control of Generation of Code ('Code Injection')	08-Mar-2025	7.2	The Allow PHP Execute plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 1.0. This is due to allowing PHP code to be entered by all users for whom unfiltered HTML is allowed. This makes it possible for authenticated attackers, with Editor-level access and above, to inject PHP code into posts and pages. **CVE ID: CVE-2024-13890**	N/A	A-SKS-ALLO-180325/138
Vendor: softdiscover					
Product: zigaform					
Affected Version(s): * Up to (excluding) 7.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	7.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in softdiscover Zigaform – Price Calculator & Cost Estimation Form Builder Lite allows Stored XSS. This issue affects Zigaform – Price Calculator & Cost Estimation Form Builder Lite: from n/a through 7.4.2.	N/A	A-SOF-ZIGA-180325/139

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-26994		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	7.1	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in softdiscover Zigaform – Form Builder Lite allows Stored XSS. This issue affects Zigaform – Form Builder Lite: from n/a through 7.4.2. **CVE ID: CVE-2025-26989**	N/A	A-SOF-ZIGA-180325/140
Vendor: spicethemes					
Product: newscrunch					
Affected Version(s): * Up to (excluding) 1.8.4.1					
Missing Authorization	04-Mar-2025	9.8	The Newscrunch theme for WordPress is vulnerable to arbitrary file uploads due to a missing capability check in the newscrunch_install_and_activate_plugin() function in all versions up to, and including, 1.8.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID: CVE-2025-1307**	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=261789%40newscrunch&new=261789%40newscrunch&sfp_email=&sfph_mail=	A-SPI-NEWS-180325/141
Cross-Site Request Forgery (CSRF)	04-Mar-2025	8.8	The Newscrunch theme for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.8.4. This is due to missing or incorrect nonce validation on the newscrunch_install_and_activate_plugin() function. This makes it possible for unauthenticated attackers to upload arbitrary files via a forged request granted they can trick a site administrator	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=261789%40newscrunch&new=261789%40newscrunch&sfp_email=&sfph_mail=	A-SPI-NEWS-180325/142

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			into performing an action such as clicking on a link. **CVE ID: CVE-2025-1306**		
Vendor: starsea99					
Product: starsea-mall					
Affected Version(s): 1.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2025	3.5	A vulnerability, which was classified as problematic, has been found in StarSea99 starsea-mall 1.0. This issue affects some unknown processing of the file /admin/goods/update. The manipulation of the argument goodsName leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2087**	N/A	A-STA-STAR-180325/143
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2025	3.5	A vulnerability classified as problematic was found in StarSea99 starsea-mall 1.0. This vulnerability affects unknown code of the file /admin/indexConfigs/update. The manipulation of the argument redirectUrl leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2086**	N/A	A-STA-STAR-180325/144
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Mar-2025	3.5	A vulnerability classified as problematic has been found in StarSea99 starsea-mall 1.0. This affects an unknown part of the file /admin/carousels/save. The manipulation of the argument redirectUrl leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has	N/A	A-STA-STAR-180325/145

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been disclosed to the public and may be used. **CVE ID: CVE-2025-2085**		
Vendor: tal					
Product: url					
Affected Version(s): * Up to (excluding) 0.11.3					
Improper Removal of Sensitive Information Before Storage or Transfer	04-Mar-2025	3.2	In the URI gem before 1.0.3 for Ruby, the URI handling methods (URI.join, URI#merge, URI#+) have an inadvertent leakage of authentication credentials because userinfo is retained even after changing the host. **CVE ID: CVE-2025-27221**	N/A	A-TAL-URL-180325/146
Affected Version(s): From (including) 0.12.0 Up to (excluding) 0.12.4					
Improper Removal of Sensitive Information Before Storage or Transfer	04-Mar-2025	3.2	In the URI gem before 1.0.3 for Ruby, the URI handling methods (URI.join, URI#merge, URI#+) have an inadvertent leakage of authentication credentials because userinfo is retained even after changing the host. **CVE ID: CVE-2025-27221**	N/A	A-TAL-URL-180325/147
Affected Version(s): From (including) 0.13.0 Up to (excluding) 0.13.2					
Improper Removal of Sensitive Information Before Storage or Transfer	04-Mar-2025	3.2	In the URI gem before 1.0.3 for Ruby, the URI handling methods (URI.join, URI#merge, URI#+) have an inadvertent leakage of authentication credentials because userinfo is retained even after changing the host. **CVE ID: CVE-2025-27221**	N/A	A-TAL-URL-180325/148
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.0.3					
Improper Removal of Sensitive Information Before Storage or Transfer	04-Mar-2025	3.2	In the URI gem before 1.0.3 for Ruby, the URI handling methods (URI.join, URI#merge, URI#+) have an inadvertent leakage of authentication credentials	N/A	A-TAL-URL-180325/149

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			because userinfo is retained even after changing the host. **CVE ID: CVE-2025-27221**		
Vendor: themesgrove					
Product: all-in-one_addons_for_elementor					
Affected Version(s): * Up to (including) 2.5.4					
Exposure of Sensitive Information to an Unauthorized Actor	08-Mar-2025	4.3	The All-in-One Addons for Elementor – WidgetKit plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.5.4 in elements/advanced-tab/template/view.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data. **CVE ID: CVE-2024-10321**	N/A	A-THE-ALL--180325/150
Vendor: tychesoftwares					
Product: product_input_fields_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.12.2					
Unrestricted Upload of File with Dangerous Type	08-Mar-2025	8.1	The Product Input Fields for WooCommerce plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the add_product_input_fields_to_order_item_meta() function in all versions up to, and including, 1.12.0. This may make it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. Please note that by default the plugin is only vulnerable to a double extension file upload attack, unless an administrators leaves the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=3234567%40product-input-fields-for-woocommerce&new=3234567%40product-input-fields-for-woocommerce&sfp_email=&sfph_mail=	A-TYC-PROD-180325/151

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accepted file extensions field blank which can make .php file uploads possible. Please note 1.12.2 was mistakenly marked as patched while 1.12.1 was marked as vulnerable for a short period of time, this is not the case and 1.12.1 is fully patched. **CVE ID: CVE-2024-13359**		
Vendor: uxper					
Product: golo					
Affected Version(s): * Up to (excluding) 1.6.11					
Missing Authorization	07-Mar-2025	9.8	The Golo - City Travel Guide WordPress Theme theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 1.6.10. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account. **CVE ID: CVE-2024-12876**	N/A	A-UXP-GOLO-180325/152
Vendor: vanokhin					
Product: shortcodes_ultimate					
Affected Version(s): * Up to (excluding) 7.3.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	6.4	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'src' parameter in all versions up to, and including, 7.3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated	https://plugins.trac.wordpress.org/changeset/3229060/	A-VAN-SHOR-180325/153

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2025-0370**		
Vendor: Vmware					
Product: cloud_foundation					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-CLOU-180325/154
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-CLOU-180325/155
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process.	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-CLOU-180325/156

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-22226		
Product: fusion					
Affected Version(s): From (including) 13.0.0 Up to (excluding) 13.6.3					
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-FUSI-180325/157
Product: telco_cloud_infrastructure					
Affected Version(s): 2.2					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/158
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/159
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-	https://support.broadcom.com/web/ecx/support-content-	A-VMW-TELC-180325/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	notification/-/external/content/SecurityAdvisories/0/25390	
Affected Version(s): 2.5					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/161
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/162
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/163
Affected Version(s): 2.7					

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
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/164
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/165
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/166
Affected Version(s): 3.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/167

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine's VMX process running on the host. **CVE ID: CVE-2025-22224**		
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/168
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/169
Product: telco_cloud_platform					
Affected Version(s): 2.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/170
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX	https://support.broadcom.com/web/ecx/support-content-notification/-	A-VMW-TELC-180325/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	/external/content/SecurityAdvisories/0/25390	
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/172
Affected Version(s): 2.5					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/173
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/174
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-	https://support.broadcom.com/web/ecx/support-content-	A-VMW-TELC-180325/175

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	notification/-/external/content/SecurityAdvisories/0/25390	
Affected Version(s): 2.7					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/176
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/177
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/178
Affected Version(s): 3.0					

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
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/179
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/180
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/181
Affected Version(s): 4.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/182

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			machine's VMX process running on the host. **CVE ID: CVE-2025-22224**		
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/183
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/184
Affected Version(s): 4.0.1					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/185
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an	https://support.broadcom.com/web/ecx/support-content-notification/-/external/conte	A-VMW-TELC-180325/186

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	nt/SecurityAdvisories/0/25390	
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/187
Affected Version(s): 5.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/188
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-TELC-180325/189
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A	https://support.broadcom.com/web/ecx/support-content-notification/-	A-VMW-TELC-180325/190

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	/external/content/SecurityAdvisories/0/25390	
Product: workstation					
Affected Version(s): From (including) 17.0 Up to (excluding) 17.6.3					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-WORK-180325/191
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	A-VMW-WORK-180325/192
Vendor: vwthemes					
Product: vw_storefront					
Affected Version(s): * Up to (excluding) 1.0.0					
Missing Authorization	04-Mar-2025	4.3	The VW Storefront theme for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the vw_storefront_reset_all_sett	https://themes.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=261535%40vw-	A-VWT-VW_S-180325/193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ings() function in all versions up to, and including, 0.9.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to reset the themes settings. **CVE ID: CVE-2024-13686**	storefront&new=261535%40vw-storefront&sfp_email=&sfph_mail=	
Vendor: wegia					
Product: wegia					
Affected Version(s): * Up to (excluding) 3.2.10					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Mar-2025	6.1	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Stored Cross-Site Scripting (XSS) vulnerability was identified in the processa_edicao_socio.php endpoint of the WeGIA application. This vulnerability allows attackers to inject malicious scripts into the socio_nome parameter. The injected scripts are stored on the server and executed automatically whenever the affected page is accessed by users, posing a significant security risk. This vulnerability is fixed in 3.2.10. **CVE ID: CVE-2025-27499**	https://github.com/LabRedesCefetRJ/WeGIA/commit/1ac0d0701ad93103482374e8092ad1a5ab15d3fc, https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-v248-mr5r-87pf, https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-v248-mr5r-87pf	A-WEG-WEGI-180325/194
Affected Version(s): * Up to (excluding) 3.2.16					
Allocation of Resources Without Limits or Throttling	03-Mar-2025	7.5	WeGIA is an open source Web Manager for Institutions with a focus on Portuguese language users. A Denial of Service (DoS) vulnerability exists in WeGIA. This vulnerability allows any unauthenticated user to cause the server to become unresponsive by performing aggressive spidering. The vulnerability	https://github.com/LabRedesCefetRJ/WeGIA/commit/624ddfadb3fd8f8b30ad4f601b032a9bacc86a39, https://github.com/LabRedesCefetRJ/WeGIA/security/advisorie	A-WEG-WEGI-180325/195

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
			is caused by recursive crawling of dynamically generated URLs and insufficient handling of large volumes of requests. This vulnerability is fixed in 3.2.16. **CVE ID: CVE-2025-27419**	s/GHSA-9rp6-4mqp-g4p8	
Vendor: wpdeveloper					
Product: essential_blocks					
Affected Version(s): * Up to (excluding) 5.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Mar-2025	6.4	The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Parallax slider in all versions up to, and including, 5.3.1 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-2025-1664**	https://plugins.trac.wordpress.org/changeset/3250957/essential-blocks/tags/5.3.2/assets/blocks/parallax-slider/frontend.js	A-WPD-ESSE-180325/196
Vendor: wpexpertplugins					
Product: post_meta_data_manager					
Affected Version(s): * Up to (including) 1.4.3					
Improper Privilege Management	08-Mar-2025	7.2	The Post Meta Data Manager plugin for WordPress is vulnerable to multisite privilege escalation in all versions up to, and including, 1.4.3. This is due to the plugin not properly verifying the existence of a multisite installation prior to allowing user meta to be added/modified. This makes it possible for authenticated attackers, with	N/A	A-WPE-POST-180325/197

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Administrator-level access and above, to gain elevated privileges on subsites that would otherwise be inaccessible. **CVE ID: CVE-2024-13835**		
Vendor: wpexperts					
Product: post_smtp					
Affected Version(s): * Up to (excluding) 3.1.3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	08-Mar-2025	4.9	The Post SMTP plugin for WordPress is vulnerable to generic SQL Injection via the 'columns' parameter in all versions up to, and including, 3.1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. **CVE ID: CVE-2024-13844**	https://plugins.trac.wordpress.org/changeset/3249371/	A-WPE-POST-180325/198
Vendor: wpfactory					
Product: wishlist_for_woocommerce					
Affected Version(s): * Up to (excluding) 3.1.8					
Cross-Site Request Forgery (CSRF)	08-Mar-2025	6.1	The Wishlist for WooCommerce: Multi Wishlists Per Customer plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.7. This is due to missing or incorrect nonce validation on the 'save_to_multiple_wishlist' function. This makes it possible for	N/A	A-WPF-WISH-180325/199

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13774**		
Vendor: wpgeodirectory					
Product: events_calendar*					
Affected Version(s): * Up to (excluding) 2.3.15					
Deserialization of Untrusted Data	03-Mar-2025	8.8	Deserialization of Untrusted Data vulnerability in Stiofan Events Calendar for GeoDirectory allows Object Injection. This issue affects Events Calendar for GeoDirectory: from n/a through 2.3.14. **CVE ID: CVE-2025-26967**	N/A	A-WPG-EVEN-180325/200
Vendor: wpsc-plugin					
Product: structured_content					
Affected Version(s): * Up to (excluding) 1.6.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Mar-2025	6.4	The Structured Content (JSON-LD) #wpsc plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sc_fs_local_business shortcode in all versions up to, and including, 6.4.5 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 accesses an injected page. **CVE ID: CVE-2025-0512**	https://plugins.trac.wordpress.org/changeset/3248930/	A-WPS-STRU-180325/201
Vendor: wpswings					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wallet_system_for_woocommerce					
Affected Version(s): * Up to (excluding) 2.6.3					
Cross-Site Request Forgery (CSRF)	04-Mar-2025	4.3	The Wallet System for WooCommerce – Wallet, Wallet Cashback, Refunds, Partial Payment, Wallet Restriction plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.2. This is due to missing or incorrect nonce validation in class-wallet-user-table.php. This makes it possible for unauthenticated attackers to modify wallet balances via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID: CVE-2024-13682**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3244479%40wallet-system-for-woocommerce%2Ftrunk&old=3231275%40wallet-system-for-woocommerce%2Ftrunk&sfp_email=&sfph_mail=	A-WPS-WALL-180325/202
Improper Authorization	04-Mar-2025	4.3	The Wallet System for WooCommerce – Wallet, Wallet Cashback, Refunds, Partial Payment, Wallet Restriction plugin for WordPress is vulnerable to unauthorized access to functionality in all versions up to, and including, 2.6.2. This makes it possible for unauthenticated attackers to increase their own wallet balance, transfer balances between arbitrary users and initiate transfer requests from other users' wallets. **CVE ID: CVE-2024-13724**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=3244479%40wallet-system-for-woocommerce%2Ftrunk&old=3231275%40wallet-system-for-woocommerce%2Ftrunk&sfp_email=&sfph_mail=	A-WPS-WALL-180325/203
Vendor: wpxpro					
Product: xpro_addons_for_elementor					
Affected Version(s): * Up to (excluding) 1.4.6.8					
Improper Neutralization of Input	08-Mar-2025	6.4	The 140+ Widgets | Xpro Addons For Elementor – FREE plugin for WordPress	https://plugins.trac.wordpress.org/changeset?sf	A-WPX-XPRO-180325/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			is vulnerable to Stored Cross-Site Scripting via several widgets in all versions up to, and including, 1.4.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. **CVE ID: CVE-2024-13649**	p_email=&sfph_mail=&reponame=&old=3235058%40xpro-elementor-addons&new=3235058%40xpro-elementor-addons&sfp_email=&sfph_mail=	
Vendor: xunruicms					
Product: xunruicms					
Affected Version(s): * Up to (including) 4.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Mar-2025	2.4	A vulnerability was found in dayrui XunRuiCMS up to 4.6.3. It has been rated as problematic. This issue affects some unknown processing of the component Friendly Links Handler. The manipulation of the argument Website Address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-2131**	N/A	A-XUN-XUNR-180325/205
Vendor: Xwiki					
Product: confluence_migrator					
Affected Version(s): * Up to (excluding) 1.11.7					
Exposure of Sensitive Information to an Unauthorized Actor	07-Mar-2025	7.5	XWiki Confluence Migrator Pro helps admins to import confluence packages into their XWiki instance. The homepage of the application is public which enables a guest to download the package which might contain sensitive	https://github.com/xwikisas/application-confluence-migrator-pro/commit/6ced42b1f341fd0ce6734fc58c7d694da5f365fb,	A-XWI-CONF-180325/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information. This vulnerability is fixed in 1.11.7. **CVE ID: CVE-2025-27604**	https://github.com/xwikisas/application-confluence-migrator-pro/security/advisories/GHSA-3w9f-2pph-j5vc	
Hardware					
Vendor: Dlink					
Product: dap-1562					
Affected Version(s): *					
Improper Resource Shutdown or Release	03-Mar-2025	6.5	A vulnerability, which was classified as critical, was found in D-Link DAP-1562 1.10. This affects the function pure_auth_check of the component HTTP POST Request Handler. The manipulation of the argument a1 leads to null pointer dereference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID: CVE-2025-1877**	N/A	H-DLI-DAP--180325/207
Vendor: espressif					
Product: esp32					
Affected Version(s): -					
Hidden Functionality	08-Mar-2025	6.8	Espressif ESP32 chips allow 29 hidden HCI commands, such as 0xFC02 (Write memory). **CVE ID: CVE-2025-27840**	N/A	H-ESP-ESP3-180325/208
Vendor: I-drive					
Product: i11					
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
N/A	03-Mar-2025	3.1	A vulnerability has been found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This vulnerability affects unknown code of the component WiFi. The manipulation leads to use of default password. Access to the local network is required for this attack to succeed. The complexity of an attack is rather high. The exploitation appears to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1878**	N/A	H-I-D-I11-180325/209
Improper Access Control	03-Mar-2025	5	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been rated as critical. Affected by this issue is some unknown functionality of the component Device Setting Handler. The manipulation leads to improper access control for register interface. The attack needs to be done within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1882**	N/A	H-I-D-I11-180325/210
Incorrect Privilege Assignment	03-Mar-2025	4.3	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Video	N/A	H-I-D-I11-180325/211

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Footage/Live Video Stream. The manipulation leads to improper access controls. The attack can be launched remotely. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1881**		
Use of Hard-coded Password	03-Mar-2025	2.4	A vulnerability was found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This issue affects some unknown processing of the component APK. The manipulation leads to hard-coded credentials. It is possible to launch the attack on the physical device. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1879**	N/A	H-I-D-I11-180325/212
Improper Authenticati on	03-Mar-2025	2	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been classified as problematic. Affected is an unknown function of the component Device Pairing. The manipulation leads to authentication bypass by primary weakness. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitability is told to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1880**	https://vuldb.com/?submit.510951	H-I-D-I11-180325/213

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: i12					
Affected Version(s): -					
N/A	03-Mar-2025	3.1	A vulnerability has been found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This vulnerability affects unknown code of the component WiFi. The manipulation leads to use of default password. Access to the local network is required for this attack to succeed. The complexity of an attack is rather high. The exploitation appears to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1878**	N/A	H-I-D-I12-180325/214
Improper Access Control	03-Mar-2025	5	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been rated as critical. Affected by this issue is some unknown functionality of the component Device Setting Handler. The manipulation leads to improper access control for register interface. The attack needs to be done within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1882**	N/A	H-I-D-I12-180325/215
Incorrect Privilege Assignment	03-Mar-2025	4.3	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been declared as problematic. Affected by this	N/A	H-I-D-I12-180325/216

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is an unknown functionality of the component Video Footage/Live Video Stream. The manipulation leads to improper access controls. The attack can be launched remotely. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1881**		
Use of Hard-coded Password	03-Mar-2025	2.4	A vulnerability was found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This issue affects some unknown processing of the component APK. The manipulation leads to hard-coded credentials. It is possible to launch the attack on the physical device. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1879**	N/A	H-I-D-I12-180325/217
Improper Authentication	03-Mar-2025	2	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been classified as problematic. Affected is an unknown function of the component Device Pairing. The manipulation leads to authentication bypass by primary weakness. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitability is told to be difficult. It was not possible to identify the current maintainer of the product. It	https://vuldb.com/?submit.510951	H-I-D-I12-180325/218

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 be assumed that the product is end-of-life. **CVE ID: CVE-2025-1880**		
Vendor: Qualcomm					
Product: 205					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-205-180325/219
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-205-180325/220
Product: 215					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-215-180325/221
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-215-180325/222
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-215-180325/223
Product: 315_5g_iot					
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
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-315_-180325/224
Product: 315_5g_iot_modem					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-315_-180325/225
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-315_-180325/226
Product: 9205_lte					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-9205-180325/227
Product: apq8017					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-APQ8-180325/228
Product: aqt1000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	H-QUA-AQT1-180325/229

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AQT1-180325/230
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AQT1-180325/231
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AQT1-180325/232
Product: ar8031					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/233
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/234
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/235
Product: ar8035					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/236
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/237
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/238
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/239
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/240
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/241
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/242

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
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/243
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/244
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-AR80-180325/245
Product: c-v2x_9150					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-C-V2-180325/246
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-C-V2-180325/247
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-C-V2-180325/248
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-C-V2-180325/249

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: csr8811					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSR8-180325/250
Product: csra6620					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/251
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/252
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/253
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/254
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/255

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/256
Product: csra6640					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/257
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/258
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/259
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/260
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRA-180325/261
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-CSRA-180325/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: csrb31024					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-CSRB-180325/263
Product: fastconnect_6200					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/264
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/265
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/266
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/267
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/268

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/269
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/270
Product: fastconnect_6700					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/271
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/272
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/273
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/274
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-FAST-180325/275

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/276
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/277
Product: fastconnect_6800					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/278
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/279
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/280
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/281
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-FAST-180325/282

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/283
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/284
Product: fastconnect_6900					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/285
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/286
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/287
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/288
Use of Out-of-range	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters	https://docs.qualcomm.com/product/publicres	H-QUA-FAST-180325/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset			are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/290
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/291
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/292
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/293
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/294
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/295
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-FAST-180325/296

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/297
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/299
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/300
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/301
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/302
Product: fastconnect_7800					
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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/303
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/304
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/305
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/306
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/307
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/308
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/309

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/310
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/311
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/312
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/313
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/314
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/315
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/316

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/317
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/318
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/319
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/320
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FAST-180325/321
Product: flight_rb5_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FLIG-180325/322
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-FLIG-180325/323

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
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FLIG-180325/324
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FLIG-180325/325
Product: fsm10056					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FSM1-180325/326
Product: fsm20055					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FSM2-180325/327
Product: fsm20056					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-FSM2-180325/328
Product: immersive_home_214					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/329
Product: immersive_home_216					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/330
Product: immersive_home_316					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/331
Product: immersive_home_318					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/332
Product: immersive_home_3210					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/333
Product: immersive_home_326					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IMME-180325/334
Product: ipq5010					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/335
Product: ipq5028					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/336
Product: ipq5300					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/337
Product: ipq5302					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/338
Product: ipq5312					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/339
Product: ipq5332					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ5-180325/340
Product: ipq6000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ6-180325/341
Product: ipq6010					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ6-180325/342
Product: ipq6018					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ6-180325/343
Product: ipq6028					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ6-180325/344
Product: ipq8070a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/345
Product: ipq8071a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/346
Product: ipq8072a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/347
Product: ipq8074a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/348
Product: ipq8076					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/349
Product: ipq8076a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/350
Product: ipq8078					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/351
Product: ipq8078a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/352
Product: ipq8173					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/353
Product: ipq8174					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ8-180325/354
Product: ipq9008					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ9-180325/355
Product: ipq9048					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ9-180325/356
Product: ipq9554					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ9-180325/357
Product: ipq9570					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ9-180325/358
Product: ipq9574					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-IPQ9-180325/359
Product: mdm9205s					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/360
Product: mdm9628					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/361
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/363
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/364
Product: mdm9640					
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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/365
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MDM9-180325/366
Product: msm8996au					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MSM8-180325/367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MSM8-180325/368
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-MSM8-180325/369
Product: pmp8074					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-PMP8-180325/370
Product: qam8255p					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/371
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/372
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/373
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/374
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/375
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/376
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/377

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/378
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/379
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/380
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/381
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/383
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/384
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-QAM8-180325/385

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Product: qam8295p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/386
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/387
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/388
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/389
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/390
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/391

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/392
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/393
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/394
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/395
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/396
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/397
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/398

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/400
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/401
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/402
Product: qam8620p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/403
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/404
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QAM8-180325/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/406
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/407
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/408
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/409
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/410
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/411
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/412

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/413
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/414
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/415
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/416
Product: qam8650p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/417
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/418
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QAM8-180325/419

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/420
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/421
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/422
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/423
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/424
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/425
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/426

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
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/427
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/428
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/429
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/430
Product: qam8775p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/431
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/432
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QAM8-180325/433

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/434
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/435
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/436
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/437
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/438
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/439
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/440

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
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/441
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/442
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/443
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/444
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAM8-180325/445
Product: qamsrv1h					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/446
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QAMS-180325/447

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/448
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/449
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/450
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/451
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/452
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/453
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/454

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/455
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/456
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/457
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/458
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/459
Product: qamsrv1m					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/460
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QAMS-180325/461

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
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/462
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/463
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/464
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/465
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/466
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/467
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/468

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/469
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/470
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/471
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/472
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QAMS-180325/473
Product: qca0000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA0-180325/474
Product: qca4004					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicres	H-QUA-QCA4-180325/475

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 lead to information disclosure. **CVE ID: CVE-2024-38426**	ources/security bulletin/march-2025-bulletin.html	
Product: qca4024					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA4-180325/476
Product: qca6174a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/477
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/478
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/479
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/480
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/481

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/482
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/483
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/484
Product: qca6175a					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/485
Product: qca6310					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/486
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/487

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/488
Product: qca6320					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/489
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/490
Product: qca6335					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/491
Product: qca6391					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/492
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/493

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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/494
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/495
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/496
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/497
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/498
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/499
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/500
Product: qca6420					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/501
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/502
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/503
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/504
Product: qca6421					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/505
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/506
Product: qca6426					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/507
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/508
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/510
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/511
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/512
Product: qca6430					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/513

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/514
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/515
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/516
Product: qca6431					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/517
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/518
Product: qca6436					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/519

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/520
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/522
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/523
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/524
Product: qca6554a					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/525
Product: qca6564					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180325/526

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/528
Product: qca6564a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/529
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/530
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/531
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/532
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-QCA6-180325/533

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
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/534
Product: qca6564au					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/535
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/536
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/537
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/538
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/539

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/540
Product: qca6574					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/541
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/542
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/543
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/544
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/545
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/546

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
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/547
Product: qca6574a					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/548
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/549
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/550
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/551
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/552
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180325/553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/554
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/555
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/556
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/557
Product: qca6574au					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/558
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/559
Time-of-check Time-of-use	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-180325/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			device due to guest VM interaction. **CVE ID: CVE-2024-53032**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/561
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/562
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/563
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/564
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/565
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/566
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/567

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
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/568
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/569
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/571
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/572
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/573
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/574

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: qca6584					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/575
Product: qca6584au					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/576
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/577
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/578
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/579
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/580

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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/581
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/582
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/583
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/584
Product: qca6595					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/585
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/586
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/588
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/589
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/590
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/591
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/592
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/593
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/595
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/596
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/597
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/598
Product: qca6595au					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/599
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/600
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/601

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/602
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/603
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/604
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/605
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/606
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/607
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/608

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/610
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/611
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/612
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/613
Product: qca6678aq					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/614
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/615

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/616
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/617
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/618
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/619
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/620
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/621
Product: qca6688aq					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180325/622

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/623
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/624
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/625
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/626
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/627
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/628
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/629

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/630
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/632
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/633
Product: qca6696					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/634
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/635
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180325/636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53030	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/637
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/638
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/639
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/640
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/641
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/642
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/643

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/644
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/645
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/646
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/647
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/648
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/649
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/650

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/651
Product: qca6698aq					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/652
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/653
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/654
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/655
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/656
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-180325/657

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
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/658
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/659
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/660
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/661
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/662
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/663
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/664

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
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/665
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/666
Product: qca6777aq					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/667
Product: qca6787aq					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/668
Product: qca6797aq					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/669
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA6-180325/670

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/671
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/672
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/674
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/675
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA6-180325/676
Product: qca8072					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA8-180325/677

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Product: qca8075					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/678
Product: qca8081					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/679
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/680
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/681
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/682
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/683

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/684
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/685
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/686
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/687
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/688
Product: qca8082					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/689
Product: qca8084					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-QCA8-180325/690

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Product: qca8085					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/691
Product: qca8337					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/692
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/693
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/694
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/695
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA8-180325/696

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/697
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/698
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/699
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/700
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/701
Product: qca8386					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA8-180325/702
Product: qca9367					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/703
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/704
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/705
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/706
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/707
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/708
Product: qca9377					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA9-180325/709

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/710
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/711
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/712
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/713
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/714
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/715
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCA9-180325/716

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: qca9888					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/717
Product: qca9889					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCA9-180325/718
Product: qcc2073					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC2-180325/719
Product: qcc2076					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC2-180325/720
Product: qcc710					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCC7-180325/721

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53023	2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/722
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/723
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/724
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/726
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/727
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/728

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/729
Product: qcc711					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCC7-180325/730
Product: qcf8000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCF8-180325/731
Product: qcf8000sfp					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCF8-180325/732
Product: qcf8001					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCF8-180325/733
Product: qcm2150					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/734
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/735
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/736
Product: qcm2290					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/737
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/738
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/739
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCM2-180325/740

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM2-180325/741
Product: qcm4290					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/742
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/744
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/745
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/746
Product: qcm4325					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/747
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/748
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/749
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/750
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/751
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/752
Product: qcm4490					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCM4-180325/753

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/754
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/755
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/756
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM4-180325/757
Product: qcm5430					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM5-180325/758
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM5-180325/759
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM5-180325/760

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM5-180325/761
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM5-180325/762
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM5-180325/763
Product: qcm6125					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/764
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/765
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/766
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-QCM6-180325/767

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/768
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/769
Product: qcm6490					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/770
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/771
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/772
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/773

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/774
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM6-180325/775
Product: qcm8550					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/776
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/777
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/778
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/779
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCM8-180325/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/781
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCM8-180325/782
Product: qcn5021					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/783
Product: qcn5022					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/784
Product: qcn5024					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/785
Product: qcn5052					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/786
Product: qcn5054					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/787
Product: qcn5122					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/788
Product: qcn5124					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/789
Product: qcn5152					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/790
Product: qcn5154					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/791
Product: qcn5164					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN5-180325/792
Product: qcn6023					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/793
Product: qcn6024					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/794
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/795
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/796

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/798
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/799
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/800
Product: qcn6100					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/801
Product: qcn6102					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/802
Product: qcn6112					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/803
Product: qcn6122					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/804
Product: qcn6132					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/805
Product: qcn6224					
Affected Version(s): *					
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/806
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/807
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/808

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/809
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/810
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/811
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/812
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/813
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/814
Product: qcn6274					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCN6-180325/815

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/816
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/817
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/818
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/819
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/820
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/821
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/822

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/823
Product: qcn6402					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/824
Product: qcn6412					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/825
Product: qcn6422					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/826
Product: qcn6432					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN6-180325/827
Product: qcn7606					
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
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN7-180325/828
Product: qcn9000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/829
Product: qcn9011					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/830
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/831
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/832
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/833
Product: qcn9012					
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
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/834
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/835
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/836
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/837
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/838
Product: qcn9022					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/839
Product: qcn9024					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-QCN9-180325/840

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/841
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/842
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/844
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/845
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/846
Product: qcn9070					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/847
Product: qcn9072					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/848
Product: qcn9074					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/849
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/850
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/851
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/852
Product: qcn9100					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/853
Product: qcn9160					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/854
Product: qcn9274					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/855
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/857
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCN9-180325/858
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/product/publicres	H-QUA-QCN9-180325/859

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	ources/security bulletin/march-2025-bulletin.html	
Product: qcs2290					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS2-180325/860
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS2-180325/861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS2-180325/862
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS2-180325/863
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS2-180325/864
Product: qcs410					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCS4-180325/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/866
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/867
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/868
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/869
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/870
Product: qcs4290					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/871
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCS4-180325/872

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/873
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/874
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/875
Product: qcs4490					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/876
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/877
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/878
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	H-QUA-QCS4-180325/879

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/880
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS4-180325/881
Product: qcs5430					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS5-180325/882
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS5-180325/883
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS5-180325/884
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS5-180325/885
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-QCS5-180325/886

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS5-180325/887
Product: qcs610					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/888
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/889
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/890
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/891
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/892

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/893
Product: qcs6125					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/894
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/895
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/896
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/897
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/898
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCS6-180325/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: qcs615					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/900
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/901
Product: qcs6490					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/902
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/903
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/905

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/906
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS6-180325/907
Product: qcs7230					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS7-180325/908
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS7-180325/909
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS7-180325/910
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS7-180325/911
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QCS7-180325/912

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS7-180325/913
Product: qcs8155					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/914
Product: qcs8250					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/915
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/916
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/917
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/918

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/919
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/920
Product: qcs8300					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/922
Product: qcs8550					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/923
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/924
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-QCS8-180325/925

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/926
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/927
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/929
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/930
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS8-180325/931
Product: qcs9100					
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
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS9-180325/932
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS9-180325/933
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS9-180325/934
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS9-180325/935
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QCS9-180325/936
Product: qdu1000					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/937
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QDU1-180325/938

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/939
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/940
Product: qdu1010					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/941
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/942
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/943
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/944
Product: qdu1110					
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
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/945
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/946
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/947
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/948
Product: qdu1210					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/949
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/950
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QDU1-180325/951

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDU1-180325/952
Product: qdx1010					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/953
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/954
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/955
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/956
Product: qdx1011					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/957

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/958
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/959
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QDX1-180325/960
Product: qep8111					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/961
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/962
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/963
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QEP8-180325/964

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/965
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/966
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QEP8-180325/967
Product: qfw7114					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/968
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/969
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/970
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QFW7-180325/971

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/972
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/973
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/974
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/975
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/976
Product: qfw7124					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/977
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a	https://docs.qualcomm.com/product/publicres	H-QUA-QFW7-180325/978

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable during extended back to back tests. **CVE ID: CVE-2024-53023**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/979
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/980
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/981
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/982
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/983
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QFW7-180325/984
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-QFW7-180325/985

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: qmp1000					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QMP1-180325/986
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QMP1-180325/987
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QMP1-180325/988
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QMP1-180325/989
Product: qrb5165m					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/990
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/991

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/992
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/993
Product: qrb5165n					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/994
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/995
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/996
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRB5-180325/997
Product: qru1032					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a	https://docs.qualcomm.com/product/publicres	H-QUA-QRU1-180325/998

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable during extended back to back tests. **CVE ID: CVE-2024-53023**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/999
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1000
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1001
Product: qru1052					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1002
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1003
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1005
Product: qru1062					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1006
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1007
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1008
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QRU1-180325/1009
Product: qsm8250					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1010
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-QSM8-180325/1011

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1012
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1013
Product: qsm8350					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1014
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1015
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1016
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QSM8-180325/1017
Product: qts110					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QTS1-180325/1018
Product: qxm8083					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-QXM8-180325/1019
Product: robotics_rb2					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1020
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1021
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1022
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1023

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1024
Product: robotics_rb3					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1025
Product: robotics_rb5					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1026
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1027
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1028
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-ROBO-180325/1029
Product: sa2150p					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA21-180325/1030
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA21-180325/1031
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA21-180325/1032
Product: sa4150p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1033
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1034
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1035
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA41-180325/1036

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: sa4155p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1037
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1039
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA41-180325/1040
Product: sa6145p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1041
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1042

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1043
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1044
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1045
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1046
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1047
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1048
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1049

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1050
Product: sa6150p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1051
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1052
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1053
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1054
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1055
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA61-180325/1056

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43061	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1058
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1059
Product: sa6155					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1060
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1061
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1062
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA61-180325/1063

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1064
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1065
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1066
Product: sa6155p					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1067
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1068
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1069
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-SA61-180325/1070

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1071
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1072
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1073
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1074
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1076
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA61-180325/1077

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA61-180325/1078
Product: sa7255p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1079
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1080
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1081
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1082
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1083
Time-of-check Time-of-use	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual	https://docs.qualcomm.com/product/publicres	H-QUA-SA72-180325/1084

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			device due to guest VM interaction. **CVE ID: CVE-2024-53032**	ources/security bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1085
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1086
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1087
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1088
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1090
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA72-180325/1091

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA72-180325/1092
Product: sa7775p					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1093
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1094
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1095
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1096
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1097
Time-of-check Time-of-use (TOCTOU)	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA77-180325/1098

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			**CVE ID: CVE-2024-53028**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1099
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1100
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1101
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1102
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1104
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA77-180325/1105

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA77-180325/1106
Product: sa8145p					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1107
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1108
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1109
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1110
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1111
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-SA81-180325/1112

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1113
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1114
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1115
Product: sa8150p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1116
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1117
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1118

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1119
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1120
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1121
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1123
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1124
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1125
Product: sa8155					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1126
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1127
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1128
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1130
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1131
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1132

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sa8155p					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1133
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1134
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1135
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1136
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1137
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1138
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA81-180325/1139

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1140
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1141
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1142
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1143
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1144
Product: sa8195p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1145
Time-of-check Time-of-use (TOCTOU)	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA81-180325/1146

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			**CVE ID: CVE-2024-53028**	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1147
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1148
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1149
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1150
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1151
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1152
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA81-180325/1153

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43060	2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1154
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA81-180325/1155
Product: sa8255p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1156
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1157
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1158
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1159
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA82-180325/1160

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53029	bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1161
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1162
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1163
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1164
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1165
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1166
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA82-180325/1167

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1168
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1169
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1170
Product: sa8295p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1171
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1172
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1173
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA82-180325/1174

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53030	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1175
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1176
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1177
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1178
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1179
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1180
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA82-180325/1181

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1182
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1183
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1185
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1186
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA82-180325/1187
Product: sa8530p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	H-QUA-SA85-180325/1188

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1189
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1190
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1191
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1192
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1193
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1194
Product: sa8540p					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1195
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1196
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1197
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1198
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1199
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1200
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1201

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1202
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1203
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1204
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1205
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1206
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1208

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1209
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA85-180325/1210
Product: sa8620p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1211
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1212
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1213
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1214
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA86-180325/1215

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1216
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1217
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1218
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1219
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1220
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1221
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1222

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1223
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1224
Product: sa8650p					
Affected Version(s): *					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1225
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1226
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1227
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1228
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA86-180325/1229

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1230
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1231
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1232
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1233
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1234
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1236

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1237
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA86-180325/1238
Product: sa8770p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1239
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1240
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1241
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1242
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA87-180325/1243

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1244
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1245
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1246
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1247
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1248
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1249
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1250

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1251
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1252
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1253
Product: sa8775p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1254
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1255
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1256
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA87-180325/1257

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1258
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1259
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1260
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1261
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1262
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1263
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1264

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1265
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1266
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1267
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA87-180325/1268
Product: sa9000p					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1269
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1270
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SA90-180325/1271

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1272
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1273
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1274
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1275
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1276
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1277
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43061		
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1279
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1280
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1281
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1282
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1283
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1284
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SA90-180325/1285

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sc8180x-aaab					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1286
Product: sc8180x-acaf					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1287
Product: sc8180x-ad					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1288
Product: sc8180xp-aaab					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1289
Product: sc8180xp-acaf					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sc8180xp-ad					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC81-180325/1291
Product: sc8280xp-abbb					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC82-180325/1292
Product: sc8380xp					
Affected Version(s): *					
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC83-180325/1293
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC83-180325/1294
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SC83-180325/1295
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SC83-180325/1296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43056	2025-bulletin.html	
Product: sd460					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD46-180325/1297
Product: sd660					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD66-180325/1298
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD66-180325/1299
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD66-180325/1300
Product: sd662					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD66-180325/1301
Product: sd670					
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
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1302
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1303
Product: sd675					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1304
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1305
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1306
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD67-180325/1307
Product: sd730					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-SD73-180325/1308

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD73-180325/1309
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD73-180325/1310
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD73-180325/1311
Product: sd835					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD83-180325/1312
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD83-180325/1313
Product: sd855					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SD85-180325/1314

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD85-180325/1315
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD85-180325/1316
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD85-180325/1317
Product: sd865_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD86-180325/1318
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD86-180325/1319
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD86-180325/1320
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SD86-180325/1321

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD86-180325/1322
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD86-180325/1323
Product: sd888					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD88-180325/1324
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD88-180325/1325
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD88-180325/1326
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD88-180325/1327
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	H-QUA-SD88-180325/1328

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Product: sdm429w					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1329
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1330
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1331
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1332
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1333
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1334

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1335
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1336
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1337
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1338
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1340
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1341

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDM4-180325/1342
Product: sdx55					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1343
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1344
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1345
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1346
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1347
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SDX5-180325/1348

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: sdx57m					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1349
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX5-180325/1350
Product: sdx61					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1351
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1352
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1353
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1354

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1355
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1356
Product: sdx65m					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX6-180325/1357
Product: sdx71m					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX7-180325/1358
Product: sdx80m					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX8-180325/1359
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SDX8-180325/1360

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426		
Product: sd_675					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_6-180325/1361
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_6-180325/1362
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_6-180325/1363
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_6-180325/1364
Product: sd_8cx					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1365
Product: sd_8_gen1_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SD_8-180325/1366

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1368
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1369
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1370
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SD_8-180325/1371
Product: sg4150p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1372
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SG41-180325/1373

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1374
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1376
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1377
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG41-180325/1378
Product: sg8275p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG82-180325/1379
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	H-QUA-SG82-180325/1380

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG82-180325/1381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG82-180325/1382
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG82-180325/1383
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SG82-180325/1384
Product: sm4125					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM41-180325/1385
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM41-180325/1386

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM41-180325/1387
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM41-180325/1388
Product: sm4635					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM46-180325/1389
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM46-180325/1390
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM46-180325/1391
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM46-180325/1392
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SM46-180325/1393

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM46-180325/1394
Product: sm6250					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM62-180325/1395
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM62-180325/1396
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM62-180325/1397
Product: sm6370					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM63-180325/1398
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM63-180325/1399

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM63-180325/1400
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM63-180325/1401
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM63-180325/1402
Product: sm6650					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1403
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1404
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1405
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SM66-180325/1406

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1407
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1408
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM66-180325/1409
Product: sm7250p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM72-180325/1410
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM72-180325/1411
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM72-180325/1412
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM72-180325/1413

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM72-180325/1414
Product: sm7315					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1415
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1416
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1417
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1418
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1419
Product: sm7325p					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1420
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1421
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1422
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1423
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM73-180325/1424
Product: sm7635					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1425
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SM76-180325/1426

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1427
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1428
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1429
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1430
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1431
Product: sm7675					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1432
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM76-180325/1433

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1435
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1436
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1437
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1438
Product: sm7675p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1439
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	H-QUA-SM76-180325/1440

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1441
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1442
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1443
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1444
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM76-180325/1445
Product: sm8550p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1446

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1447
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1448
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1449
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1450
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1451
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM85-180325/1452
Product: sm8635					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SM86-180325/1453

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1454
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1455
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1456
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1457
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1458
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1459
Product: sm8635p					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM86-180325/1460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1461
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1463
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1464
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1465
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1466
Product: sm8650q					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-SM86-180325/1467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1468
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1469
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1470
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1471
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1472
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM86-180325/1473
Product: sm8735					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1474
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1475
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1476
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1477
Product: sm8750					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1478
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1479
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SM87-180325/1480

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1481
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1482
Product: sm8750p					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1483
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1484
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1485
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SM87-180325/1486
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM87-180325/1487

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53025	bulletin/march-2025-bulletin.html	
Product: smart_audio_400					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1488
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1489
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1490
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1491
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1492
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SMAR-180325/1493
Product: snapdragon_210					
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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1494
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1495
Product: snapdragon_212					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1496
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1497
Product: snapdragon_429					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1498
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1499
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1500

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1501
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1502
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1503
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1504
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1505
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1506
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1507

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1508
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1509
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1510
Product: snapdragon_429_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1511
Product: snapdragon_439					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1512
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1513

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1514
Product: snapdragon_460					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1515
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1516
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1518
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1519
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: snapdragon_460_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1521
Product: snapdragon_480\+_5g					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1522
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1523
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1525
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1526

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1527
Product: snapdragon_480_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1528
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1529
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1531
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1532
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: snapdragon_4_gen_1					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1534
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1535
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1536
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1537
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1538
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1539
Product: snapdragon_4_gen_2					
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
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1540
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1542
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1543
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1544
Product: snapdragon_660					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1545
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1546

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1547
Product: snapdragon_662					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1548
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1549
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1550
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1551
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1552
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 lead to information disclosure. **CVE ID: CVE-2024-38426**	bulletin/march-2025-bulletin.html	
Product: snapdragon_662_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1554
Product: snapdragon_665					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1555
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1556
Product: snapdragon_670					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1557
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1558
Product: snapdragon_675					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1559
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1560
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1561
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1562
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1563
Product: snapdragon_678					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1564
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1565

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1566
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1567
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1568
Product: snapdragon_680_4g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1569
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1570
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1571
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1572

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1573
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1574
Product: snapdragon_680_4g_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1575
Product: snapdragon_685_4g					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1576
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1577
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1578

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1579
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1580
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1581
Product: snapdragon_685_4g_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1582
Product: snapdragon_690_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1583
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1584

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1585
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1586
Product: snapdragon_695_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1587
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1588
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1590
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1592
Product: snapdragon_710					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1593
Product: snapdragon_720g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1594
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1595
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1596
Product: snapdragon_730					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1597

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1598
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1599
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1600
Product: snapdragon_730g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1601
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1602
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1603
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure. **CVE ID: CVE-2024-38426**	bulletin/march-2025-bulletin.html	
Product: snapdragon_732g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1605
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1606
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1607
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1608
Product: snapdragon_750g_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1609
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1611
Product: snapdragon_765g_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1612
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1613
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1614
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1615
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1616
Product: snapdragon_765_5g					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1617
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1618
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1619
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1620
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1621
Product: snapdragon_768g_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1622
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1623

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1624
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1625
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1626
Product: snapdragon_778g\+_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1627
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1628
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1629
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1630

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1631
Product: snapdragon_778g_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1632
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1633
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1635
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1636
Product: snapdragon_780g_5g					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1637
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1638
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1640
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1641
Product: snapdragon_782g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1642
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1643

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1645
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1646
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1647
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1648
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1649
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1651
Product: snapdragon_820_automotive					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1653
Product: snapdragon_835_mobile_pc					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1654
Product: snapdragon_835_pc					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1655
Product: snapdragon_845					
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
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1656
Product: snapdragon_850					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1657
Product: snapdragon_855					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1658
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1659
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1660
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1661
Product: snapdragon_855\+					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1662
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1663
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1664
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1665
Product: snapdragon_860					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1666
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1667
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1668

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1669
Product: snapdragon_8657+_5g					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1670
Product: snapdragon_865\+_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1671
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1672
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1674

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1675
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1676
Product: snapdragon_865_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1677
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1678
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1679
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1680
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1681

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1682
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1683
Product: snapdragon_870_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1684
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1685
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1686
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1687
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1688

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1689
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1690
Product: snapdragon_888\+_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1691
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1692
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1693
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1694
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1695

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1696
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1697
Product: snapdragon_888_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1698
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1699
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1700
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1701

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1702
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1703
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1704
Product: snapdragon_8cx_gen_3_compute					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1705
Product: snapdragon_8\+_gen_1					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1706
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1707
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1709
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1710
Product: snapdragon_8\+_gen_2					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1711
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1712
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1713
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1714

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1715
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1716
Product: snapdragon_8\+_gen_2_mobile					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1717
Product: snapdragon_8_gen_1					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1718
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1719
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1720
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1721

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1722
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1724
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1725
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1726
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1727
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1728

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: snapdragon_8_gen_2					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1729
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1730
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1732
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1733
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1734
Product: snapdragon_8_gen_2_mobile					
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
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1735
Product: snapdragon_8_gen_3					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1736
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1737
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1738
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1739
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1740
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1741

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1742
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1743
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1744
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1745
Product: snapdragon_ar1_gen_1					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1746
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1747
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SNAP-180325/1748

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1749
Product: snapdragon_ar1_gen_1_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1750
Product: snapdragon_ar2_gen_1					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1751
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1752
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1754

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1755
Product: snapdragon_ar2_gen_1_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1756
Product: snapdragon_auto_4g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1757
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1758
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1759
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1760
Product: snapdragon_auto_5g					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1761
Product: snapdragon_auto_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1762
Product: snapdragon_auto_5g-rf_gen_2					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1763
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1765
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1766

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_auto_5g_modem-rf_gen_2					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1767
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1768
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1770
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1771
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1772
Product: snapdragon_w5\+_gen_1					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1774
Product: snapdragon_w5\+_gen_1_wearable					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1775
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1776
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1777
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1778
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1779

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1780
Product: snapdragon_wear_1300					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1781
Product: snapdragon_wear_4100\+					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1782
Product: snapdragon_wear_4100\+_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1783
Product: snapdragon_x12_lte					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1784
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1785

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Improper Authenticati on	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1786
Product: snapdragon_x24_lte					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1787
Product: snapdragon_x35_5g					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1788
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1789
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1790
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1791

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1792
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1793
Product: snapdragon_x35_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1794
Product: snapdragon_x50_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1795
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1796
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1797

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1798
Product: snapdragon_x55_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1799
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1800
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1802
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1803
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1804

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: snapdragon_x55_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1805
Product: snapdragon_x5_lte					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1806
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1807
Product: snapdragon_x62_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1808
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1809
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1810

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1811
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1812
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1813
Product: snapdragon_x62_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1814
Product: snapdragon_x65_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1815
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1816

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1817
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1818
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1819
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1820
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1821
Product: snapdragon_x65_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1822
Product: snapdragon_x70-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1823

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 lead to information disclosure. **CVE ID: CVE-2024-38426**	ources/security bulletin/march-2025-bulletin.html	
Product: snapdragon_x72_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1824
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1825
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1826
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1827
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1829
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-SNAP-180325/1830

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1831
Product: snapdragon_x72_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1832
Product: snapdragon_x75_5g					
Affected Version(s): *					
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1833
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1834
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1835
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SNAP-180325/1836

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53023	2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1838
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1839
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1840
Product: snapdragon_x75_5g-rf					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1841
Product: snapdragon_xr1					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1842

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1843
Product: snapdragon_xr2\+_gen_1					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1844
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1845
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1846
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1847
Product: snapdragon_xr2_5g					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1848
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-180325/1849

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1850
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1851
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1852
Product: snapdragon_xr2_5g_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SNAP-180325/1853
Product: srv1h					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1854
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SRV1-180325/1855

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1856
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1857
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1858
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1859
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1860
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1861
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1862

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1863
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1864
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1865
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1866
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1867
Product: srv1l					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1868
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SRV1-180325/1869

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1870
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1871
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1872
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1873
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1874
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1875
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1876

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1877
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1879
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1880
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1881
Product: srv1m					
Affected Version(s): *					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1882
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SRV1-180325/1883

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1884
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1885
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1886
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1887
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1888
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1889
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1890

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1891
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1893
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1894
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SRV1-180325/1895
Product: ssg2115p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1896
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SSG2-180325/1897

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1898
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1899
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1900
Product: ssg2125p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1901
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1902
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1903
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SSG2-180325/1904

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SSG2-180325/1905
Product: sw5100					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1906
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1907
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1908
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1909
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1910
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-SW51-180325/1911

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1912
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1913
Product: sw5100p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1914
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1915
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1916
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1917

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1919
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1920
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SW51-180325/1921
Product: sxr1120					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1922
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1923
Product: sxr1230p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL	https://docs.qualcomm.com/product/publicres	H-QUA-SXR1-180325/1924

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	ources/security bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1925
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1926
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1927
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR1-180325/1928
Product: sxr2130					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1929
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1930

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1931
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1932
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1933
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1934
Product: sxr2230p					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1935
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1936
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SXR2-180325/1937

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1938
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1939
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1940
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1941
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1942
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1943
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-SXR2-180325/1944

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-49836	2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1945
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1946
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1947
Product: sxr2250p					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1948
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1949
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1950
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SXR2-180325/1951

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1952
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1953
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1954
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1955
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1956
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1957
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SXR2-180325/1958

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1959
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1960
Product: sxr2330p					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1961
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1962
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1963
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1964
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-SXR2-180325/1965

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1966
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-SXR2-180325/1967
Product: talynplus					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-TALY-180325/1968
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-TALY-180325/1969
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-TALY-180325/1970
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-TALY-180325/1971
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-TALY-180325/1972

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Product: video_collaboration_vc1					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1973
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1974
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1975
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1976
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1977
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1979
Product: video_collaboration_vc3					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1980
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1981
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1982
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1983
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1984
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-VIDE-180325/1985

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1986
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1987
Product: video_collaboration_vc5					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1988
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1989
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1990
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1991
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-VIDE-180325/1992

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VIDE-180325/1993
Product: vision_intelligence_300_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VISI-180325/1994
Product: vision_intelligence_400					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VISI-180325/1995
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VISI-180325/1996
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-VISI-180325/1997
Product: vision_intelligence_400_					
Affected Version(s): *					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-VISI-180325/1998

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Product: wcd9306					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/1999
Product: wcd9326					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2000
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2002
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2003
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2004

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2005
Product: wcd9330					
Affected Version(s): *					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2006
Product: wcd9335					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2007
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2008
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2009
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2010
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	H-QUA-WCD9-180325/2011

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2012
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2013
Product: wcd9340					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2014
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2015
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2016
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2017
Use of Out-of-range	03-Mar-2025	7.8	Memory corruption during voice activation, when	https://docs.qualcomm.com/pr	H-QUA-WCD9-180325/2018

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset			sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2019
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2020
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2021
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2022
Product: wcd9341					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2023
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2024

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2025
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2026
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2028
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2029
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2030
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2031
Product: wcd9360					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2032
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2033
Product: wcd9370					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2034
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2035
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2036
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2037
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCD9-180325/2038

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2039
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2040
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2041
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2042
Product: wcd9371					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2043
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2044
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-180325/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure. **CVE ID: CVE-2024-38426**	bulletin/march-2025-bulletin.html	
Product: wcd9375					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2046
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2047
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2048
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2050
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2051
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-WCD9-180325/2052

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2053
Product: wcd9378					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2054
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2055
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2056
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2057
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2058

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2059
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2060
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2061
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2062
Product: wcd9380					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2063
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2064
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCD9-180325/2065

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2066
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2067
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2068
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2069
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2070
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2071
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-180325/2072

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43062	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2073
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2074
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2075
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2076
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2077
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2078
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCD9-180325/2079

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2080
Product: wcd9385					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2081
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2082
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2083
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2084
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2085

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2086
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2087
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2088
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2089
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2090
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2091
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2092

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2093
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2095
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2096
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2097
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2098
Product: wcd9390					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCD9-180325/2099

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2100
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2101
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2102
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2103
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2104
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2105
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2106

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2107
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2108
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2109
Product: wcd9395					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2110
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2111
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2112
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCD9-180325/2113

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2114
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2116
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2117
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2118
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2119
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCD9-180325/2120

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcn3610					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2121
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2122
Product: wcn3615					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2123
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2124
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2125
Product: wcn3620					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2126

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2127
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2128
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2129
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2130
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2131
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2132
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2133

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2134
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2135
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2137
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2138
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2139
Product: wcn3660b					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN3-180325/2140

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2141
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2142
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2143
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2144
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2145
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2146
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN3-180325/2147

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2148
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2149
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2150
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2152
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2153
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2154

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcn3680					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2155
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2156
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2157
Product: wcn3680b					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2158
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2159
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2160
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL	https://docs.qualcomm.com/product/publicres	H-QUA-WCN3-180325/2161

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2162
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2163
Product: wcn3910					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2164
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2165
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2166
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2167

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2168
Product: wcn3950					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2169
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2170
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2171
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2172
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2173
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN3-180325/2174

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2175
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2176
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2177
Product: wcn3980					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2178
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2179
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2180
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180325/2181

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2183
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2184
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2185
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2186
Product: wcn3988					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2187
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	H-QUA-WCN3-180325/2188

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2189
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2190
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2192
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2193
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2194
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN3-180325/2195

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: wcn3990					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2196
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2197
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2198
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2199
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2200
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2201
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN3-180325/2202

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 lead to information disclosure. **CVE ID: CVE-2024-38426**	bulletin/march-2025-bulletin.html	
Product: wcn3999					
Affected Version(s): *					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN3-180325/2203
Product: wcn6450					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2204
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2205
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2206
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2207
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN6-180325/2208

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2209
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2210
Product: wcn6650					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2211
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2212
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2214
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN6-180325/2215

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2216
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2217
Product: wcn6740					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2218
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2219
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2220
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2221
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	H-QUA-WCN6-180325/2222

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Product: wcn6755					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2223
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2224
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2225
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2226
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2227
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2228
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-WCN6-180325/2229

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN6-180325/2230
Product: wcn7750					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2231
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2232
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2233
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2234
Product: wcn7860					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WCN7-180325/2235

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45580	2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2236
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2237
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2238
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2239
Product: wcn7861					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2240
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2241
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCN7-180325/2242

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2243
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2244
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2245
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2246
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2247
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2248
Product: wcn7880					
Affected Version(s): *					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	H-QUA-WCN7-180325/2249

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2250
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2251
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2252
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2253
Product: wcn7881					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2254
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2255
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL	https://docs.qualcomm.com/pr	H-QUA-WCN7-180325/2256

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2257
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2258
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2259
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2260
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2261
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WCN7-180325/2262
Product: wsa8810					
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
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2263
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2264
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2265
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2266
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2267
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2268
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2269
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	H-QUA-WSA8-180325/2270

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2271
Product: wsa8815					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2272
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2273
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2274
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2275
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2277
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2278
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2279
Product: wsa8830					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2280
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2281
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2282
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WSA8-180325/2283

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2284
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2285
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2286
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2287
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2288
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2289
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2290

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43061		
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2291
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2292
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2293
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2294
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2295
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2296
Product: wsa8832					
Affected Version(s): *					
Buffer Copy without Checking Size of Input	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180325/2297

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-43055**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2298
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2299
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2300
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2301
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2302
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2303
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WSA8-180325/2304

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2305
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2306
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2308
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2309
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2310
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2311

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2312
Product: wsa8835					
Affected Version(s): *					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2313
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2314
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2315
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2316
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2317
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WSA8-180325/2318

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43061	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2319
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2320
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2321
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2322
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2323
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2325

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2326
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2327
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2328
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2329
Product: wsa8840					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2330
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2331
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WSA8-180325/2332

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2333
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2334
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2335
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2336
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2337
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2338
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	H-QUA-WSA8-180325/2339

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2340
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2341
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2342
Product: wsa8845					
Affected Version(s): *					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2343
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2344
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2345
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180325/2346

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53023	bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2347
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2348
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2349
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2351
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2352
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-180325/2353

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2354
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2355
Product: wsa8845h					
Affected Version(s): *					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2356
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2357
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2358
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2359
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a	https://docs.qualcomm.com/product/publicres	H-QUA-WSA8-180325/2360

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable during extended back to back tests. **CVE ID: CVE-2024-53023**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2361
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2362
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2364
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2365
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2366
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/product/publicres	H-QUA-WSA8-180325/2367

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	ources/security bulletin/march-2025-bulletin.html	
Improper Authenticati on	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	H-QUA-WSA8-180325/2368
Vendor: Tenda					
Product: ac6					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Mar-2025	8.8	A vulnerability, which was classified as critical, has been found in Tenda AC6 15.03.05.16. Affected by this issue is some unknown functionality of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1814**	N/A	H-TEN-AC6-180325/2369
Product: ac8					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Mar-2025	8.8	A vulnerability was found in Tenda AC8 16.03.34.06 and classified as critical. This issue affects the function sub_49E098 of the file /goform/SetIpMacBind of the component Parameter Handler. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1853**	N/A	H-TEN-AC8-180325/2370

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: tx3					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability classified as critical has been found in Tenda TX3 16.03.13.11_multi. This affects an unknown part of the file /goform/setMacFilterCfg. The manipulation of the argument deviceList leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1895**	N/A	H-TEN-TX3-180325/2371
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability classified as critical was found in Tenda TX3 16.03.13.11_multi. This vulnerability affects unknown code of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1896**	N/A	H-TEN-TX3-180325/2372
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability, which was classified as critical, has been found in Tenda TX3 16.03.13.11_multi. This issue affects some unknown processing of the file /goform/SetNetControlList. The manipulation of the argument list leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1897**	N/A	H-TEN-TX3-180325/2373
Improper Restriction of	04-Mar-2025	6.5	A vulnerability, which was classified as critical, was found in Tenda TX3	N/A	H-TEN-TX3-180325/2374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			16.03.13.11_multi. Affected is an unknown function of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime/schedEndTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1898**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability has been found in Tenda TX3 16.03.13.11_multi and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1899**	N/A	H-TEN-TX3-180325/2375
Operating System					
Vendor: Apple					
Product: ipados					
Affected Version(s): * Up to (excluding) 18.0					
Uncontrolled Resource Consumption	10-Mar-2025	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID: CVE-2024-44227**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121250	O-APP-IPAD-180325/2376
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is	https://support.apple.com/en-us/121238, https://support.	O-APP-IPAD-180325/2377

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	
Exposure of Sensitive Information to an Unauthorized Actor	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15, macOS Sonoma 14.7, visionOS 2, iOS 18 and iPadOS 18. A local user may be able to leak sensitive user information. **CVE ID: CVE-2024-54469**	https://support.apple.com/en-us/121234, https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121247, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-IPAD-180325/2378
N/A	10-Mar-2025	5.5	A logic issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, tvOS 18, macOS Sequoia 15. A malicious app may be able to modify other apps without having App Management permission. **CVE ID: CVE-2024-54560**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121250	O-APP-IPAD-180325/2379
Affected Version(s): * Up to (excluding) 18.3.2					
Out-of-bounds Write	11-Mar-2025	8.8	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web	https://support.apple.com/en-us/122281, https://support.apple.com/en-us/122283, https://support.apple.com/en-us/122284,	O-APP-IPAD-180325/2380

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). **CVE ID: CVE-2025-24201**	https://support.apple.com/en-us/122285	
Product: iphone_os					
Affected Version(s): * Up to (excluding) 18.0					
Uncontrolled Resource Consumption	10-Mar-2025	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID: CVE-2024-44227**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121250	O-APP-IPHO-180325/2381
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-IPHO-180325/2382
Exposure of Sensitive Information to an	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15, macOS Sonoma	https://support.apple.com/en-us/121234, https://support.apple.com/en-	O-APP-IPHO-180325/2383

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			14.7, visionOS 2, iOS 18 and iPadOS 18. A local user may be able to leak sensitive user information. **CVE ID: CVE-2024-54469**	us/121238, https://support.apple.com/en-us/121247, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	
N/A	10-Mar-2025	5.5	A logic issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, tvOS 18, macOS Sequoia 15. A malicious app may be able to modify other apps without having App Management permission. **CVE ID: CVE-2024-54560**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121250	O-APP-IPHO-180325/2384
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-IPHO-180325/2385
Affected Version(s): * Up to (excluding) 18.3.2					
Out-of-bounds Write	11-Mar-2025	8.8	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web content may be able to break	https://support.apple.com/en-us/122281, https://support.apple.com/en-us/122283, https://support.apple.com/en-us/122284, https://support.	O-APP-IPHO-180325/2386

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). **CVE ID: CVE-2025-24201**	apple.com/en-us/122285	
Product: macos					
Affected Version(s): * Up to (excluding) 13.7					
Exposure of Sensitive Information to an Unauthorized Actor	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15, macOS Sonoma 14.7, visionOS 2, iOS 18 and iPadOS 18. A local user may be able to leak sensitive user information. **CVE ID: CVE-2024-54469**	https://support.apple.com/en-us/121234, https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121247, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-MACO-180325/2387
Affected Version(s): * Up to (excluding) 15.0					
Uncontrolled Resource Consumption	10-Mar-2025	7.5	The issue was addressed with improved memory handling. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to cause unexpected system termination or corrupt kernel memory. **CVE ID: CVE-2024-44227**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121250	O-APP-MACO-180325/2388
Uncontrolled Resource Consumption	10-Mar-2025	7.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An app may be able to cause unexpected system	https://support.apple.com/en-us/121238	O-APP-MACO-180325/2389

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			termination or corrupt kernel memory. **CVE ID: CVE-2024-54546**		
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-MACO-180325/2390
N/A	10-Mar-2025	5.5	This issue was addressed with improved entitlements. This issue is fixed in macOS Sequoia 15. An app may be able to access removable volumes without user consent. **CVE ID: CVE-2024-54463**	https://support.apple.com/en-us/121238	O-APP-MACO-180325/2391
Exposure of Sensitive Information to an Unauthorized Actor	10-Mar-2025	5.5	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data. **CVE ID: CVE-2024-54473**	https://support.apple.com/en-us/121238	O-APP-MACO-180325/2392
N/A	10-Mar-2025	5.5	A logic issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, tvOS 18, macOS Sequoia 15. A malicious app may be able to modify other apps without having App Management permission. **CVE ID: CVE-2024-54560**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121248, https://support.	O-APP-MACO-180325/2393

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121250	
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-MACO-180325/2394
Affected Version(s): * Up to (excluding) 15.3.2					
Out-of-bounds Write	11-Mar-2025	8.8	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). **CVE ID: CVE-2025-24201**	https://support.apple.com/en-us/122281, https://support.apple.com/en-us/122283, https://support.apple.com/en-us/122284, https://support.apple.com/en-us/122285	O-APP-MACO-180325/2395
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7					
Exposure of Sensitive Information to an	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15, macOS Sonoma	https://support.apple.com/en-us/121234, https://support.apple.com/en-	O-APP-MACO-180325/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			14.7, visionOS 2, iOS 18 and iPadOS 18. A local user may be able to leak sensitive user information. **CVE ID: CVE-2024-54469**	us/121238, https://support.apple.com/en-us/121247, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	
Product: tvos					
Affected Version(s): * Up to (excluding) 18.0					
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-TVOS-180325/2397
N/A	10-Mar-2025	5.5	A logic issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, tvOS 18, macOS Sequoia 15. A malicious app may be able to modify other apps without having App Management permission. **CVE ID: CVE-2024-54560**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121250	O-APP-TVOS-180325/2398
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-	O-APP-TVOS-180325/2399

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	
Product: visionos					
Affected Version(s): * Up to (excluding) 2.0					
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-VISI-180325/2400
Exposure of Sensitive Information to an Unauthorized Actor	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15, macOS Sonoma 14.7, visionOS 2, iOS 18 and iPadOS 18. A local user may be able to leak sensitive user information. **CVE ID: CVE-2024-54469**	https://support.apple.com/en-us/121234, https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121247, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-VISI-180325/2401
Affected Version(s): * Up to (excluding) 2.3.2					
Out-of-bounds Write	11-Mar-2025	8.8	An out-of-bounds write issue was addressed with improved checks to prevent unauthorized actions. This	https://support.apple.com/en-us/122281, https://support.	O-APP-VISI-180325/2402

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue is fixed in visionOS 2.3.2, iOS 18.3.2 and iPadOS 18.3.2, macOS Sequoia 15.3.2, Safari 18.3.1. Maliciously crafted web content may be able to break out of Web Content sandbox. This is a supplementary fix for an attack that was blocked in iOS 17.2. (Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals on versions of iOS before iOS 17.2.). **CVE ID: CVE-2025-24201**	apple.com/en-us/122283, https://support.apple.com/en-us/122284, https://support.apple.com/en-us/122285	
Product: watchos					
Affected Version(s): * Up to (excluding) 11.0					
N/A	10-Mar-2025	6.5	A cookie management issue was addressed with improved state management. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin. **CVE ID: CVE-2024-54467**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-WATC-180325/2403
N/A	10-Mar-2025	5.5	A logic issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, tvOS 18, macOS Sequoia 15. A malicious app may be able to modify other apps without having App Management permission. **CVE ID: CVE-2024-54560**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121248, https://support.	O-APP-WATC-180325/2404

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121250	
N/A	10-Mar-2025	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11, macOS Sequoia 15, Safari 18, visionOS 2, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID: CVE-2024-44192**	https://support.apple.com/en-us/121238, https://support.apple.com/en-us/121240, https://support.apple.com/en-us/121241, https://support.apple.com/en-us/121248, https://support.apple.com/en-us/121249, https://support.apple.com/en-us/121250	O-APP-WATC-180325/2405
Vendor: Dlink					
Product: dap-1562_firmware					
Affected Version(s): 1.10					
Improper Resource Shutdown or Release	03-Mar-2025	6.5	A vulnerability, which was classified as critical, was found in D-Link DAP-1562 1.10. This affects the function pure_auth_check of the component HTTP POST Request Handler. The manipulation of the argument a1 leads to null pointer dereference. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID: CVE-2025-1877**	N/A	O-DLI-DAP--180325/2406
Vendor: espressif					
Product: esp32_firmware					
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
Hidden Functionality	08-Mar-2025	6.8	Espressif ESP32 chips allow 29 hidden HCI commands, such as 0xFC02 (Write memory). **CVE ID: CVE-2025-27840**	N/A	O-ESP-ESP3-180325/2407
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2408
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2409
Affected Version(s): 13.0.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2410
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2411
Affected Version(s): 14.0.0					

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
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2412
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-EMUI-180325/2413
Product: harmonyos					
Affected Version(s): 2.0.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2414
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2415
Affected Version(s): 2.1.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2416

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2417
Affected Version(s): 3.0.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2418
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2419
Affected Version(s): 3.1.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2420
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2421
Affected Version(s): 4.0.0					

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
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2422
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2423
Affected Version(s): 4.2.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2424
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2425
Affected Version(s): 4.3.0					
Improper Input Validation	04-Mar-2025	8.4	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58044**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2426
N/A	04-Mar-2025	7.3	Permission bypass vulnerability in the window module	https://consumer.huawei.com/	O-HUA-HARM-180325/2427

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58043**	en/support/bulletin/2025/3/	
Affected Version(s): 5.0.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Mar-2025	8.6	Multi-concurrency vulnerability in the media digital copyright protection module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58045**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2428
N/A	04-Mar-2025	6.8	Vulnerability of improper access permission in the process management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2025-27521**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2429
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Mar-2025	6.7	Multi-thread problem vulnerability in the package management module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-58048**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2430
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-2025	6.2	Vulnerability of improper access permission in the HDC module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58050**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2431
Exposure of Sensitive Information to an	04-Mar-2025	6.2	Permission management vulnerability in the lock screen module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2432

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58046**		
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-2025	5	Permission verification vulnerability in the media library module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58049**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2433
Exposure of Sensitive Information to an Unauthorized Actor	04-Mar-2025	5	Permission verification vulnerability in the media library module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-58047**	https://consumer.huawei.com/en/support/bulletin/2025/3/	O-HUA-HARM-180325/2434
Vendor: I-drive					
Product: i11_firmware					
Affected Version(s): * Up to (including) 20250227					
Improper Access Control	03-Mar-2025	5	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been rated as critical. Affected by this issue is some unknown functionality of the component Device Setting Handler. The manipulation leads to improper access control for register interface. The attack needs to be done within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1882**	N/A	O-I-D-I11_-180325/2435

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Privilege Assignment	03-Mar-2025	4.3	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Video Footage/Live Video Stream. The manipulation leads to improper access controls. The attack can be launched remotely. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1881**	N/A	O-I-D-I11_-180325/2436
N/A	03-Mar-2025	3.1	A vulnerability has been found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This vulnerability affects unknown code of the component WiFi. The manipulation leads to use of default password. Access to the local network is required for this attack to succeed. The complexity of an attack is rather high. The exploitation appears to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1878**	N/A	O-I-D-I11_-180325/2437
Use of Hard-coded Password	03-Mar-2025	2.4	A vulnerability was found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This issue affects some unknown processing of the component APK. The manipulation leads to hard-coded credentials. It is possible to launch the attack on the physical device. It	N/A	O-I-D-I11_-180325/2438

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1879**		
Improper Authentication	03-Mar-2025	2	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been classified as problematic. Affected is an unknown function of the component Device Pairing. The manipulation leads to authentication bypass by primary weakness. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitability is told to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1880**	https://vuldb.com/?submit.510951	O-I-D-I11_-180325/2439
Product: i12_firmware					
Affected Version(s): * Up to (including) 20250227					
Improper Access Control	03-Mar-2025	5	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been rated as critical. Affected by this issue is some unknown functionality of the component Device Setting Handler. The manipulation leads to improper access control for register interface. The attack needs to be done within the local network. The complexity of an attack is rather high. The exploitation is known to be difficult. It was not possible to identify the current maintainer of the product. It	N/A	O-I-D-I12_-180325/2440

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 be assumed that the product is end-of-life. **CVE ID: CVE-2025-1882**		
Incorrect Privilege Assignment	03-Mar-2025	4.3	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Video Footage/Live Video Stream. The manipulation leads to improper access controls. The attack can be launched remotely. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1881**	N/A	O-I-D-I12_-180325/2441
N/A	03-Mar-2025	3.1	A vulnerability has been found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This vulnerability affects unknown code of the component WiFi. The manipulation leads to use of default password. Access to the local network is required for this attack to succeed. The complexity of an attack is rather high. The exploitation appears to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1878**	N/A	O-I-D-I12_-180325/2442
Use of Hard-coded Password	03-Mar-2025	2.4	A vulnerability was found in i-Drive i11 and i12 up to 20250227 and classified as problematic. This issue affects some unknown processing of the component APK. The	N/A	O-I-D-I12_-180325/2443

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation leads to hard-coded credentials. It is possible to launch the attack on the physical device. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1879**		
Improper Authentication	03-Mar-2025	2	A vulnerability was found in i-Drive i11 and i12 up to 20250227. It has been classified as problematic. Affected is an unknown function of the component Device Pairing. The manipulation leads to authentication bypass by primary weakness. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. The exploitability is told to be difficult. It was not possible to identify the current maintainer of the product. It must be assumed that the product is end-of-life. **CVE ID: CVE-2025-1880**	https://vuldb.com/?submit.510951	O-I-D-I12_-180325/2444
Vendor: Juniper					
Product: junos					
Affected Version(s): * Up to (including) 21.2					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device.	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2445

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Affected Version(s): 21.2					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6,	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2446

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Affected Version(s): 21.4					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2447
Affected Version(s): 22.2					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Affected Version(s): 22.4					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS:	https://support.portal.juniper.net/JSA93446	O-JUN-JUNO-180325/2449

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Affected Version(s): 23.2					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4,	https://support.portal.juniper.net/JSA93446	O-JUN-JUNO-180325/2450

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			* 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Affected Version(s): 23.4					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2451
Affected Version(s): 24.2					
Insufficient Compartmentalization	12-Mar-2025	4.4	An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks Junos OS allows a local attacker with high privileges to compromise the integrity of the device.	https://supportportal.juniper.net/JSA93446	O-JUN-JUNO-180325/2452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. This issue is not exploitable from the Junos CLI. This issue affects Junos OS: * All versions before 21.2R3-S9, * 21.4 versions before 21.4R3-S10, * 22.2 versions before 22.2R3-S6, * 22.4 versions before 22.4R3-S6, * 23.2 versions before 23.2R2-S3, * 23.4 versions before 23.4R2-S4, * 24.2 versions before 24.2R1-S2, 24.2R2. **CVE ID: CVE-2025-21590**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Improper Access Control	03-Mar-2025	8.5	There is an improper access control issue in ArcGIS Server versions 10.9.1 through 11.3 on Windows and Linux, which under unique circumstances, could potentially allow a remote, low privileged authenticated attacker to access secure services published a standalone (Unfederated) ArcGIS Server instance. If successful this compromise would have a high impact on Confidentiality, low impact on integrity and no impact to availability of the software.	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	O-LIN-LINU-180325/2453

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-51954		
Affected Version(s): * Up to (excluding) 5.15.176					
Improper Locking	12-Mar-2025	8.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid racy issue with session expire. **CVE ID: CVE-2024-58087**	https://git.kernel.org/stable/c/2107ab40629aeabbec369cf34b8cf0f288c3eb1b, https://git.kernel.org/stable/c/37a0e2b362b3150317fb6e2139de67b1e29ae5ff, https://git.kernel.org/stable/c/450a844c045ff0895d41b05a1cbe8febd1acfcfd	O-LIN-LINU-180325/2454
Affected Version(s): * Up to (excluding) 5.4.215					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Mar-2025	4.7	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the params_lock mutex for the rest. When the stream is set up again by another thread between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same	https://git.kernel.org/stable/c/4051324a6dafd7053c74c475e80b3ba10ae672b0, https://git.kernel.org/stable/c/723ac5ab2891b6c10dd6cc78ef5456af593490eb, https://git.kernel.org/stable/c/8015ef9e8a0ee5cecfd0cb6805834d007ab26f86	O-LIN-LINU-180325/2455

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			params_lock mutex with snd_pcm_oss_make_ready_locked() variant. **CVE ID: CVE-2022-49733**		
Affected Version(s): 4.19.73					
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double accounting race when btrfs_run_delalloc_range() failed [BUG] When running btrfs with block size (4K) smaller than page size (64K, aarch64), there is a very high chance to crash the kernel at generic/750, with the following messages: (before the call traces, there are 3 extra debug messages added) BTRFS warning (device dm-3): read-write for sector size 4096 with page size 65536 is experimental BTRFS info (device dm-3): checking UUID tree hrtimer: interrupt took 5451385 ns BTRFS error (device dm-3): cow_file_range failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): run_delalloc_nocow failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): failed to run delalloc range, root=4957 ino=257 folio=1572864 submit_bitmap=8-15	https://git.kernel.org/stable/c/0283ee1912c8e243c931f4ee5b3672e954fe0384, https://git.kernel.org/stable/c/21333148b5c9e52f41fafcedec3810b56a5e0e40, https://git.kernel.org/stable/c/72dad8e377afa50435940adfb697e070d3556670	O-LIN-LINU-180325/2456

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			start=1605632 len=69632: -28 ----------[cut here]---------- WARNING: CPU: 2 PID: 3020984 at ordered-data.c:360 can_finish_ordered_extent+0x370/0x3b8 [btrfs] CPU: 2 UID: 0 PID: 3020984 Comm: kworker/u24:1 Tainted: G OE 6.13.0-rc1-custom+ #89 Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: events_unbound btrfs_async_reclaim_data_space [btrfs] pc : can_finish_ordered_extent+0x370/0x3b8 [btrfs] lr : can_finish_ordered_extent+0x1ec/0x3b8 [btrfs] Call trace: can_finish_ordered_extent+0x370/0x3b8 [btrfs] (P) can_finish_ordered_extent+0x1ec/0x3b8 [btrfs] (L) btrfs_mark_ordered_io_finished+0x130/0x2b8 [btrfs] extent_writepage+0x10c/0x3b8 [btrfs] extent_write_cache_pages+0x21c/0x4e8 [btrfs] btrfs_writepages+0x94/0x160 [btrfs] do_writepages+0x74/0x190 filemap_fdatawrite_wbc+0x		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			74/0xa0 start_delalloc_inodes+0x17c/0x3b0 [btrfs] btrfs_start_delalloc_roots+0x17c/0x288 [btrfs] shrink_delalloc+0x11c/0x280 [btrfs] flush_space+0x288/0x328 [btrfs] btrfs_async_reclaim_data_space+0x180/0x228 [btrfs] process_one_work+0x228/0x680 worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1605632 OE len=16384 to_dec=16384 left=0 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1622016 OE len=12288 to_dec=12288 left=0 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1634304 OE len=8192 to_dec=4096 left=0 CPU: 1 UID: 0 PID: 3286940 Comm: kworker/u24:3 Tainted: G W OE 6.13.0-rc1-custom+ #89 Hardware name: QEMU		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: btrfs_work_helper [btrfs] (btrfs-endio-write) pstate: 404000c5 (nZcv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : process_one_work+0x110/0x680 lr : worker_thread+0x1bc/0x360 Call trace: process_one_work+0x110/0x680 (P) worker_thread+0x1bc/0x360 (L) worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 Code: f84086a1 f9000fe1 53041c21 b9003361 (f9400661) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception SMP: stopping secondary CPUs SMP: failed to stop secondary CPUs 2-3 Dumping ftrace buffer: (ftrace buffer empty) Kernel Offset: 0x275bb9540000 from 0xffff800080000000 PHYS_OFFSET: 0xffff8fbba0000000 CPU features: 0x100,00000070,00801250,8201720b [CAUSE] The above warning is triggered immediately after the delalloc range		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failure, this happens in the following sequence: - Range [1568K, 1636K) is dirty 1536K 1568K 1600K 1636K 1664K | |/////////\/////////| | Where 1536K, 1600K and 1664K are page boundaries (64K page size) - Enter extent_writepage() for page 1536K - Enter run_delalloc_nocow() with locke ---truncated--- **CVE ID: CVE-2024-58089**		
Affected Version(s): 5.10.211					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2457
Affected Version(s): 5.10.234					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22,	O-LIN-LINU-180325/2458

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks	https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 dev from gn->gtp_dev_list, and calls unregister_netdevice_queue (). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack fffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack fffffe8040b4f990+0x7990/0x8000 [kworker/u8:7+netns 1804]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R10: process kstack ffffffe8040b4f997+0x7997/ 0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_ core_dev_11127_8_1328_8_ S_4096_A_64_n_139+0xc08 /0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 ffffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] ffffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] ffffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): 5.15.150					

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2459
Affected Version(s): 5.15.177					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2460

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue(). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack ffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack ffffe8040b4f990+0x7990/0x8000 [kworker/u8:7+netns 1804] R10: process kstack ffffe8040b4f997+0x7997/0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc08/0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 fffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): 5.4.290					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue(). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack ffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack ffffe8040b4f990+0x7990/0x8000 [kworker/u8:7+netns 1804] R10: process kstack ffffe8040b4f997+0x7997/0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc08/0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			shadow CR4: 0000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 fffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): 6.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Mar-2025	4.7	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the params_lock mutex for the rest. When the stream is set up again by another thread	https://git.kernel.org/stable/c/4051324a6dafd7053c74c475e80b3ba10ae672b0, https://git.kernel.org/stable/c/723ac5ab2891b6c10dd6cc78ef5456af593490eb, https://git.kernel.org/stable/c/8015ef9e8a0ee5cecfd0cb6805834d007ab26f86	O-LIN-LINU-180325/2462

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same params_lock mutex with snd_pcm_oss_make_ready_locked() variant. **CVE ID: CVE-2022-49733**		
Affected Version(s): 6.13					
Improper Locking	12-Mar-2025	8.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid racy issue with session expire. **CVE ID: CVE-2024-58087**	https://git.kernel.org/stable/c/2107ab40629aeabbec369cf34b8cf0f288c3eb1b, https://git.kernel.org/stable/c/37a0e2b362b3150317fb6e2139de67b1e29ae5ff, https://git.kernel.org/stable/c/450a844c045ff0895d41b05a1cbe8febd1acfcfd	O-LIN-LINU-180325/2463
Affected Version(s): 6.14					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller reported a use-after-free in geneve_find_dev() [0] without repro. geneve_configure() links struct geneve_dev.next to net_generic(net, geneve_net_id)->geneve_list.	https://git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf, https://git.kernel.org/stable/c/5a0538ac6826807d6919f6aecbb8996c2865af2c, https://git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	O-LIN-LINU-180325/2464

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 net here could differ from dev_net(dev) if IFLA_NET_NS_PID, IFLA_NET_NS_FD, or IFLA_TARGET_NETNSID is set. When dev_net(dev) is dismantled, geneve_exit_batch_rtnl() finally calls unregister_netdevice_queue() for each dev in the netns, and later the dev is freed. However, its geneve_dev.next is still linked to the backend UDP socket netns. Then, use-after-free will occur when another geneve dev is created in the netns. Let's call geneve_dellink() instead in geneve_destroy_tunnels(). [0]: BUG: KASAN: slab-use-after-free in geneve_find_dev drivers/net/geneve.c:1295 [inline] BUG: KASAN: slab-use-after-free in geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 Read of size 2 at addr ffff000054d6ee24 by task syz.1.4029/13441 CPU: 1 UID: 0 PID: 13441 Comm: syz.1.4029 Not tainted 6.13.0-g0ad9617c78ac #24 dc35ca22c79fb82e8e7bc5c9c9adafea898b1e3d Hardware 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
			linux,dummy-virt (DT) Call trace: show_stack+0x38/0x50 arch/arm64/kernel/stacktrace.c:466 (C) __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xbc/0x108 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x16c/0x6f0 mm/kasan/report.c:489 kasan_report+0xc0/0x120 mm/kasan/report.c:602 __asan_report_load2_noabort+0x20/0x30 mm/kasan/report_generic.c:379 geneve_find_dev drivers/net/geneve.c:1295 [inline] geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 geneve_newlink+0xb8/0x128 drivers/net/geneve.c:1634 rtnl_newlink_create+0x23c/0x868 net/core/rtnetlink.c:3795 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:25		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			43 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x618/0x838 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x5fc/0x8b0 net/netlink/af_netlink.c:1892 sock_sendmsg_nosec net/socket.c:713 [inline] __sock_sendmsg net/socket.c:728 [inline] ___sys_sendmsg+0x410/0x6f8 net/socket.c:2568 __sys_sendmsg+0x178/0x1d8 net/socket.c:2622 __sys_sendmsg net/socket.c:2654 [inline] __do_sys_sendmsg net/socket.c:2659 [inline] __se_sys_sendmsg net/socket.c:2657 [inline] __arm64_sys_sendmsg+0x12c/0x1c8 net/socket.c:2657 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x90/0x278 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x13c/0x250 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x54/0x70 arch/arm64/kernel/syscall.c:151 el0_svc+0x4c/0xa8 arch/arm64/kernel/entry-		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common.c:744 el0t_64_sync_handler+0x78 /0x108 arch/arm64/kernel/entry- common.c:762 el0t_64_sync+0x198/0x1a0 arch/arm64/kernel/entry.S :600 Allocated by task 13247: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x 68 mm/kasan/common.c:68 kasan_save_alloc_info+0x44 /0x58 mm/kasan/generic.c:568 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x84/0xa 0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4298 [inline] __kmalloc_node_noprof+0x2 a0/0x560 mm/slub.c:4304 __kvmalloc_node_noprof+0x 9c/0x230 mm/util.c:645 alloc_netdev_mqs+0xb8/0x 11a0 net/core/dev.c:11470 rtnl_create_link+0x2b8/0xb 50 net/core/rtnetlink.c:3604 rtnl_newlink_create+0x19c/ 0x868 net/core/rtnetlink.c:3780 __rtnl_newlink		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_n ---truncated--- **CVE ID: CVE-2025-21858**		
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/ism: add release function for struct device According to device_release() in /drivers/base/core.c, a device without a release function is a broken device and must be fixed. The current code directly frees the device after calling device_add() without waiting for other kernel parts to release their references. Thus, a reference could still be held to a struct device, e.g., by sysfs, leading to potential use-after-free issues if a proper release function is not set. **CVE ID: CVE-2025-21856**	https://git.kernel.org/stable/c/0505ff2936f166405d81d0d454a81d9c14124344, https://git.kernel.org/stable/c/915e34d5ad35a6a9e56113f852ade4a730fb88f0, https://git.kernel.org/stable/c/940d15254d2216b585558bcf36312da50074e711	O-LIN-LINU-180325/2465

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Don't reference skb after sending to VIOS Previously, after successfully flushing the xmit buffer to VIOS, the tx_bytes stat was incremented by the length of the skb. It is invalid to access the skb memory after sending the buffer to the VIOS because, at any point after sending, the VIOS can trigger an interrupt to free this memory. A race between reading skb->len and freeing the skb is possible (especially during LPM) and will result in use-after-free: ========== ========== ========== === BUG: KASAN: slab-use-after-free in ibmvnic_xmit+0x75c/0x1808 [ibmvnic] Read of size 4 at addr c00000024eb48a70 by task hxecom/14495 <...> Call Trace: [c000000118f66cf0] [c0000000018cba6c] dump_stack_lvl+0x84/0xe8 (unreliable) [c000000118f66d20] [c0000000006f0080] print_report+0x1a8/0x7f0 [c000000118f66df0] [c0000000006f08f0] kasan_report+0x128/0x1f8 [c000000118f66f00]	https://git.kernel.org/stable/c/093b0e5c90592773863f300b908b741622eef597, https://git.kernel.org/stable/c/25dddd01dcc8ef3acff964dbb32eeb0d89f098e9, https://git.kernel.org/stable/c/501ac6a7e21b82e05207c6b4449812d82820f306	O-LIN-LINU-180325/2466

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[c0000000006f2868] __asan_load4+0xac/0xe0 [c000000118f66f20] [c0080000046eac84] ibmvnic_xmit+0x75c/0x1808 [ibmvnic] [c000000118f67340] [c0000000014be168] dev_hard_start_xmit+0x150/0x358 <...> Freed by task 0: kasan_save_stack+0x34/0x68 kasan_save_track+0x2c/0x50 kasan_save_free_info+0x64/0x108 __kasan_mempool_poison_object+0x148/0x2d4 napi_skb_cache_put+0x5c/0x194 net_tx_action+0x154/0x5b8 handle_softirqs+0x20c/0x60c do_softirq_own_stack+0x6c/0x88 <...> The buggy address belongs to the object at c00000024eb48a00 which belongs to the cache skbuff_head_cache of size 224 ========== ========== ========== === **CVE ID: CVE-2025-21855**		
N/A	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1e988c3fe1264	O-LIN-LINU-180325/2467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			io_uring: prevent opcode speculation sqe->opcode is used for different tables, make sure we santitise it against speculations. **CVE ID: CVE-2025-21863**	708f4f92109203ac5b1d65de50b, https://git.kernel.org/stable/c/506b9b5e8c2d2a411ea8fe361333f5081c56d23a, https://git.kernel.org/stable/c/b9826e3b26ec031e9063f64a7c735449c43955e4	
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: f_midi: f_midi_complete to call queue_work When using USB MIDI, a lock is attempted to be acquired twice through a re-entrant call to f_midi_transmit, causing a deadlock. Fix it by using queue_work() to schedule the inner f_midi_transmit() via a high priority work queue from the completion handler. **CVE ID: CVE-2025-21859**	https://git.kernel.org/stable/c/1f10923404705a94891e612dff3b75e828a78368, https://git.kernel.org/stable/c/24a942610ee9bafb2692a456ae850c5b2e409b05, https://git.kernel.org/stable/c/4ab37fcb42832cdd3e9d5e50653285ca84d6686f	O-LIN-LINU-180325/2468
Use After Free	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/migrate_device: don't add folio to be freed to LRU in migrate_device_finalize() If migration succeeded, we called folio_migrate_flags()->mem_cgroup_migrate() to migrate the memcg from the	https://git.kernel.org/stable/c/069dd21ea8262204f94737878389c2815a054a9e, https://git.kernel.org/stable/c/3f9240d59e9a95d19f06120bfd1d0e681c6c0ac7, https://git.kern	O-LIN-LINU-180325/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			old to the new folio. This will set memcg_data of the old folio to 0. Similarly, if migration failed, memcg_data of the dst folio is left unset. If we call folio_putback_lru() on such folios (memcg_data == 0), we will add the folio to be freed to the LRU, making memcg code unhappy. Running the hmm selftests: # ./hmm-tests ... # RUN hmm.hmm_device_private. migrate ... [102.078007][T14893] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x7ff27d200 pfn:0x13cc00 [102.079974][T14893] anon flags: 0x17ff00000020018(uptodate|dirty|swapbacked|node=0|zone=2|lastcpupid=0x7ff) [102.082037][T14893] raw: 017ff00000020018 dead000000000100 dead000000000122 ffff8881353896c9 [102.083687][T14893] raw: 00000007ff27d200 0000000000000000 00000001ffffffff 0000000000000000 [102.085331][T14893] page dumped because: VM_WARN_ON_ONCE_FOLIO(!memcg && !mem_cgroup_disabled()) [102.087230][T14893] ------------[cut here]------------ [102.088279][T14893] WARNING: CPU: 0 PID:	el.org/stable/c/41cddf83d8b00f29fd105e7a0777366edc69a5cf	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			14893 at ./include/linux/memcontrol.h:726 folio_lruvec_lock_irqsave+0x10e/0x170 [102.090478][T14893] Modules linked in: [102.091244][T14893] CPU: 0 UID: 0 PID: 14893 Comm: hmm-tests Not tainted 6.13.0-09623-g6c216bc522fd #151 [102.093089][T14893] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 [102.094848][T14893] RIP: 0010:folio_lruvec_lock_irqsave+0x10e/0x170 [102.096104][T14893] Code: ... [102.099908][T14893] RSP: 0018:ffffc900236c37b0 EFLAGS: 00010293 [102.101152][T14893] RAX: 0000000000000000 RBX: ffffea0004f30000 RCX: ffffffff8183f426 [102.102684][T14893] RDX: ffff8881063cb880 RSI: ffffffff81b8117f RDI: ffff8881063cb880 [102.104227][T14893] RBP: 0000000000000000 R08: 0000000000000005 R09: 0000000000000000 [102.105757][T14893] R10: 0000000000000001 R11: 0000000000000002 R12: ffffc900236c37d8 [102.107296][T14893] R13: ffff888277a2bcb0 R14: 000000000000001f R15: 0000000000000000 [102.108830][T14893] FS: 00007ff27dbdd740(0000) GS:ffff888277a00000(0000)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			knlGS:0000000000000000 [102.110643][T14893] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [102.111924][T14893] CR2: 00007ff27d400000 CR3: 000000010866e000 CR4: 0000000000750ef0 [102.113478][T14893] PKRU: 55555554 [102.114172][T14893] Call Trace: [102.114805][T14893] <TASK> [102.115397][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.116547][T14893] ? __warn.cold+0x110/0x210 [102.117461][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.118667][T14893] ? report_bug+0x1b9/0x320 [102.119571][T14893] ? handle_bug+0x54/0x90 [102.120494][T14893] ? exc_invalid_op+0x17/0x50 [102.121433][T14893] ? asm_exc_invalid_op+0x1a/0x20 [102.122435][T14893] ? __wake_up_klogd.part.0+0x76/0xd0 [102.123506][T14893] ? dump_page+0x4f/0x60 [102.124352][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.125500][T14893] folio_batch_move_lru+0xd4/0x200 [102.126577][T14893] ? __pfx_lru_add+0x10/0x10 [102.127505][T14893] __folio_batch_add_and_move+0x391/0x720 [102.128633][T14893] ? __pfx_lru_add+0x10/0x10 [102.129550][T14893] folio_putback_lru+0x16/0x80		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[102.130564][T14893] migrate_device_finalize+0x9b/0x530 [102.131640][T14893] dmirror_migrate_to_device.constprop.0+0x7c5/0xad0 [102.133047][T14893] dmirror_fops_unlocked_ioctl+0x89b/0xc80 Likely, nothing else goes wrong: putting the last folio reference will remove the folio from the LRU again. So besides memcg complaining, adding the folio to be freed to the LRU is just an unnecessary step. The new flow resembles what we have in migrate_folio_move(): add the dst to the lru, rem ---truncated--- **CVE ID: CVE-2025-21861**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop dst Xiumei reported hitting the WARN in xfrm6_tunnel_net_exit while running tests that boil down to: - create a pair of netns - run a basic TCP test over ipcomp6 - delete the pair of netns The xfrm_state found on spi_byaddr was not deleted at the time we delete the netns, because we still have a reference on it.	https://git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9, https://git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491, https://git.kernel.org/stable/c/9b6412e6979f6f9e0632075f8f008937b5cd4efd	O-LIN-LINU-180325/2470

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 lingering reference comes from a secpath (which holds a ref on the xfrm_state), which is still attached to an skb. This skb is not leaked, it ends up on sk_receive_queue and then gets defer-free'd by skb_attempt_defer_free. The problem happens when we defer freeing an skb (push it on one CPU's defer_list), and don't flush that list before the netns is deleted. In that case, we still have a reference on the xfrm_state that we don't expect at this point. We already drop the skb's dst in the TCP receive path when it's no longer needed, so let's also drop the secpath. At this point, tcp_filter has already called into the LSM hooks that may require the secpath, so it should not be needed anymore. However, in some of those places, the MPTCP extension has just been attached to the skb, so we cannot simply drop all extensions. **CVE ID: CVE-2025-21864**		
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b96160	O-LIN-LINU-180325/2471

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue	0ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack fffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack fffffe8040b4f990+0x7990/0x8000 [kworker/u8:7+netns 1804] R10: process kstack fffffe8040b4f997+0x7997/0x8000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_ core_dev_11127_8_1328_8_ S_4096_A_64_n_139+0xc08 /0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 fffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Allocation of Resources Without	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2d542f13d26344e3452eee7761	O-LIN-LINU-180325/2472

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			powerpc/code-patching: Fix KASAN hit by not flagging text patching area as VM_ALLOC Erhard reported the following KASAN hit while booting his PowerMac G4 with a KASAN-enabled kernel 6.13-rc6: BUG: KASAN: vmalloc-out-of-bounds in copy_to_kernel_nofault+0xd8/0x1c8 Write of size 8 at addr f1000000 by task chronyd/1293 CPU: 0 UID: 123 PID: 1293 Comm: chronyd Tainted: G W 6.13.0-rc6-PMacG4 #2 Tainted: [W]=WARN Hardware name: PowerMac3,6 7455 0x80010303 PowerMac Call Trace: [c2437590] [c1631a84] dump_stack_lvl+0x70/0x8c (unreliable) [c24375b0] [c0504998] print_report+0xdc/0x504 [c2437610] [c050475c] kasan_report+0xf8/0x108 [c2437690] [c0505a3c] kasan_check_range+0x24/0x18c [c24376a0] [c03fb5e4] copy_to_kernel_nofault+0xd8/0x1c8 [c24376c0] [c004c014] patch_instructions+0x15c/0x16c [c2437710] [c00731a8] bpf_arch_text_copy+0x60/0x7c [c2437730] [c0281168] bpf_jit_binary_pack_finalize+0x50/0xac [c2437750] [c0073cf4] bpf_int_jit_compile+0xb30/	3026ce9b653065, https://git.kernel.org/stable/c/2e6c80423f201405fd65254e52decd21663896f3, https://git.kernel.org/stable/c/6847b3e40bb963e57b61d1cc6fe84cb37b9d3d4c	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0xdec [c2437880] [c0280394] bpf_prog_select_runtime+0x15c/0x478 [c24378d0] [c1263428] bpf_prepare_filter+0xbf8/0xc14 [c2437990] [c12677ec] bpf_prog_create_from_user+0x258/0x2b4 [c24379d0] [c027111c] do_seccomp+0x3dc/0x1890 [c2437ac0] [c001d8e0] system_call_exception+0x2dc/0x420 [c2437f30] [c00281ac] ret_from_syscall+0x0/0x2c --- interrupt: c00 at 0x5a1274 NIP: 005a1274 LR: 006a3b3c CTR: 005296c8 REGS: c2437f40 TRAP: 0c00 Tainted: G W (6.13.0-rc6-PMacG4) MSR: 0200f932 <VEC,EE,PR,FP,ME,IR,DR,RI> CR: 24004422 XER: 00000000 GPR00: 00000166 af8f3fa0 a7ee3540 00000001 00000000 013b6500 005a5858 0200f932 GPR08: 00000000 00001fe9 013d5fc8 005296c8 2822244c 00b2fcd8 00000000 af8f4b57 GPR16: 00000000 00000001 00000000 00000000 00000000 00000001 00000000 00000002 GPR24: 00afdbb0 00000000 00000000 00000000 006e0004 013ce060 006e7c1c 00000001 NIP [005a1274] 0x5a1274 LR [006a3b3c] 0x6a3b3c --- interrupt: c00		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 buggy address belongs to the virtual mapping at [f1000000, f1002000) created by: text_area_cpu_up+0x20/0x190 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x76e30 flags: 0x80000000(zone=2) raw: 80000000 00000000 00000122 00000000 00000000 00000000 ffffffff 00000001 raw: 00000000 page dumped because: kasan: bad access detected Memory state around the buggy address: f0ffff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0ffff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >f1000000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ f1000080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f1000100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ========== f8 corresponds to KASAN_VMALLOC_INVALID which means the area is not initialised hence not supposed to be used yet. Powerpc text patching		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			infrastructure allocates a virtual memory area using get_vm_area() and flags it as VM_ALLOC. But that flag is meant to be used for vmalloc() and vmalloc() allocated memory is not supposed to be used before a call to __vmalloc_node_range() which is never called for that area. That went undetected until commit e4137f08816b ("mm, kasan, kmsan: instrument copy_from/to_kernel_nofault") The area allocated by text_area_cpu_up() is not vmalloc memory, it is mapped directly on demand when needed by map_kernel_page(). There is no VM flag corresponding to such usage, so just pass no flag. That way the area will be unpoisonned and usable immediately. **CVE ID: CVE-2025-21866**		
Use of Uninitialized Resource	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix incorrect initialization order Syzkaller reports the following bug: BUG: spinlock bad magic on CPU#1, syz-executor.0/7995 lock: 0xffff88805303f3e0, .magic: 00000000, .owner: <none>/-1, .owner_cpu: 0	https://git.kernel.org/stable/c/07b598c0e6f06a0f254c88dafb4ad50f8a8c6eea, https://git.kernel.org/stable/c/0efa6c42f81c60d8f72ba7f5ed8d4fec8c526282, https://git.kernel.org/stable/c/219a47d0e6195bd202f22855e35f25bd15bc4d58	O-LIN-LINU-180325/2473

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted: G E 5.10.209+ #1 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x119/0x179 lib/dump_stack.c:118 debug_spin_lock_before kernel/locking/spinlock_debug.c:83 [inline] do_raw_spin_lock+0x1f6/0x270 kernel/locking/spinlock_debug.c:112 __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:117 [inline] _raw_spin_lock_irqsave+0x50/0x70 kernel/locking/spinlock.c:159 reset_per_cpu_data+0xe6/0x240 [drop_monitor] net_dm_cmd_trace+0x43d/0x17a0 [drop_monitor] genl_family_rcv_msg_doit+0x22f/0x330 net/netlink/genetlink.c:739 genl_family_rcv_msg net/netlink/genetlink.c:783 [inline] genl_rcv_msg+0x341/0x5a0 net/netlink/genetlink.c:800 netlink_rcv_skb+0x14d/0x440 net/netlink/af_netlink.c:2497 genl_rcv+0x29/0x40 net/netlink/genetlink.c:811		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x54b/0x800 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x914/0xe00 net/netlink/af_netlink.c:1916 sock_sendmsg_nosec net/socket.c:651 [inline] __sock_sendmsg+0x157/0x190 net/socket.c:663 ____sys_sendmsg+0x712/0x870 net/socket.c:2378 ___sys_sendmsg+0xf8/0x170 net/socket.c:2432 __sys_sendmsg+0xea/0x1b0 net/socket.c:2461 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x62/0xc7 RIP: 0033:0x7f3f9815aee9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3f972bf0c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f3f9826d050 RCX: 00007f3f9815aee9 RDX: 0000000020000000 RSI: 0000000020001300 RDI: 0000000000000007		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBP: 00007f3f981b63bd R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f3f9826d050 R15: 00007ffe01ee6768 If drop_monitor is built as a kernel module, syzkaller may have time to send a netlink NET_DM_CMD_START message during the module loading. This will call the net_dm_monitor_start() function that uses a spinlock that has not yet been initialized. To fix this, let's place resource initialization above the registration of a generic netlink family. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with Syzkaller. **CVE ID: CVE-2025-21862**		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix deadlock when freeing cgroup storage The following commit bc235cdb423a ("bpf: Prevent deadlock from recursive bpf_task_storage_[get|delete]") first introduced deadlock prevention for fentry/fexit programs attaching on bpf_task_storage helpers.	https://git.kernel.org/stable/c/6ecb9fa14eec5f15d97c84c36896871335f6ddfb, https://git.kernel.org/stable/c/c78f4afbd962f43a3989f45f3ca04300252b19b5, https://git.kernel.org/stable/c/fac674d2bd68f3479f27328626b42d1eebd11fef	O-LIN-LINU-180325/2474

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			That commit also employed the logic in map free path in its v6 version. Later bpf_cgrp_storage was first introduced in c4bcfb38a95e ("bpf: Implement cgroup storage available to non-cgroup-attached bpf progs") which faces the same issue as bpf_task_storage, instead of its busy counter, NULL was passed to bpf_local_storage_map_free() which opened a window to cause deadlock: <TASK> (acquiring local_storage->lock) _raw_spin_lock_irqsave+0x3d/0x50 bpf_local_storage_update+0xd1/0x460 bpf_cgrp_storage_get+0x109/0x130 bpf_prog_a4d4a370ba857314_cgrp_ptr+0x139/0x170 ? __bpf_prog_enter_recur+0x16/0x80 bpf_trampoline_6442485186+0x43/0xa4 cgroup_storage_ptr+0x9/0x20 (holding local_storage->lock) bpf_selem_unlink_storage_nolock.constprop.0+0x135/0x160 bpf_selem_unlink_storage+0x6f/0x110 bpf_local_storage_map_free+0xa2/0x110 bpf_map_free_deferred+0x5b/0x90 process_one_work+0x17c/0x390 worker_thread+0x251/0x360		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread+0xd2/0x100 ret_from_fork+0x34/0x50 ret_from_fork_asm+0x1a/0x30 </TASK> Progs: - A: SEC("fentry/cgroup_storage_ptr") - cgid (BPF_MAP_TYPE_HASH) Record the id of the cgroup the current task belonging to in this hash map, using the address of the cgroup as the map key. - cgrpa (BPF_MAP_TYPE_CGRP_STORAGE) If current task is a kworker, lookup the above hash map using function parameter @owner as the key to get its corresponding cgroup id which is then used to get a trusted pointer to the cgroup through bpf_cgroup_from_id(). This trusted pointer can then be passed to bpf_cgrp_storage_get() to finally trigger the deadlock issue. - B: SEC("tp_btf/sys_enter") - cgrpb (BPF_MAP_TYPE_CGRP_STORAGE) The only purpose of this prog is to fill Prog A's hash map by calling bpf_cgrp_storage_get() for as many userspace		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tasks as possible. Steps to reproduce: - Run A; - while (true) { Run B; Destroy B; } Fix this issue by passing its busy counter to the free procedure so it can be properly incremented before storage/smap locking. **CVE ID: CVE-2024-58088**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2475
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mtd: spi-nor: sst: Fix SST write failure 'commit 18bcb4aa54ea ("mtd: spi-nor: sst: Factor out common write operation to `sst_nor_write_data()`")' introduced a bug where only one byte of data is written, regardless of the number of bytes passed to sst_nor_write_data(), causing a kernel crash	https://git.kernel.org/stable/c/539bd20352832b9244238a055eb169ccf1c41ff6, https://git.kernel.org/stable/c/9553391f32f8c43e12fc7c04e1035160b5ea20bf, https://git.kernel.org/stable/c/bb1accc7e0f688886f0c634f2e878b8ac4ee6a58	O-LIN-LINU-180325/2476

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			during the write operation. Ensure the correct number of bytes are written as passed to sst_nor_write_data(). Call trace: [57.400180] ------------[cut here]------------ [57.404842] While writing 2 byte written 1 bytes [57.409493] WARNING: CPU: 0 PID: 737 at drivers/mtd/spi-nor/sst.c:187 sst_nor_write_data+0x6c/0x74 [57.418464] Modules linked in: [57.421517] CPU: 0 UID: 0 PID: 737 Comm: mtd_debug Not tainted 6.12.0-g5ad04afd91f9 #30 [57.429517] Hardware name: Xilinx Versal A2197 Processor board revA - x-prc-02 revA (DT) [57.437600] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [57.444557] pc : sst_nor_write_data+0x6c/0x74 [57.448911] lr : sst_nor_write_data+0x6c/0x74 [57.453264] sp : ffff80008232bb40 [57.456570] x29: ffff80008232bb40 x28: 0000000000010000 x27: 0000000000000001 [57.463708] x26: 000000000000ffff x25: 0000000000000000 x24: 0000000000000000 [57.470843] x23: 0000000000010000 x22: ffff80008232bbf0 x21: ffff000816230000 [57.477978] x20:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff0008056c0080 x19: 0000000000000002 x18: 0000000000000006 [57.485112] x17: 0000000000000000 x16: 0000000000000000 x15: ffff80008232b580 [57.492246] x14: 0000000000000000 x13: ffff8000816d1530 x12: 00000000000004a4 [57.499380] x11: 000000000000018c x10: ffff8000816fd530 x9 : ffff8000816d1530 [57.506515] x8 : 00000000fffff7ff x7 : ffff8000816fd530 x6 : 0000000000000001 [57.513649] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [57.520782] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0008049b0000 [57.527916] Call trace: [57.530354] sst_nor_write_data+0x6c/0x74 [57.534361] sst_nor_write+0xb4/0x18c [57.538019] mtd_write_oob_std+0x7c/0x88 [57.541941] mtd_write_oob+0x70/0xbc [57.545511] mtd_write+0x68/0xa8 [57.548733] mtdchar_write+0x10c/0x290 [57.552477] vfs_write+0xb4/0x3a8 [57.555791] ksys_write+0x74/0x10c [57.559189] __arm64_sys_write+0x1c/0x28 [57.563109] invoke_syscall+0x54/0x11c		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[57.566856] el0_svc_common.constprop.0+0xc0/0xe0 [57.571557] do_el0_svc+0x1c/0x28 [57.574868] el0_svc+0x30/0xcc [57.577921] el0t_64_sync_handler+0x120/0x12c [57.582276] el0t_64_sync+0x190/0x194 [57.585933] ---[end trace 0000000000000000]--- [pratyush@kernel.org: add Cc stable tag] **CVE ID: CVE-2025-21845**		
Use of Uninitialized Resource	07-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: avoid garbage value in panthor_ioctl_dev_query() 'priorities_info' is uninitialized, and the uninitialized value is copied to user object when calling PANTHOR_UOBJ_SET(). Using memset to initialize 'priorities_info' to avoid this garbage value problem. **CVE ID: CVE-2025-21843**	https://git.kernel.org/stable/c/3b32b7f638fe61e9d2929096017 2f4e360e38233, https://git.kernel.org/stable/c/64b95bbc08bacf3e4b05c8604e6a4fec43bb712a	O-LIN-LINU-180325/2477
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: sockmap, vsock: For connectible sockets allow only connected sockmap expects all vsocks to have a transport assigned, which is expressed in vsock_proto::psock_update_sk_prot(). However, there is	https://git.kernel.org/stable/c/22b683217ad2112791a708693cb236507abd637a, https://git.kernel.org/stable/c/8fb5bb169d17cdd12c2dcc2e96830ed487d77a0f, https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an edge case where an unconnected (connectible) socket may lose its previously assigned transport. This is handled with a NULL check in the vsock/BPF recv path. Another design detail is that listening vsocks are not supposed to have any transport assigned at all. Which implies they are not supported by the sockmap. But this is complicated by the fact that a socket, before switching to TCP_LISTEN, may have had some transport assigned during a failed connect() attempt. Hence, we may end up with a listening vsock in a sockmap, which blows up quickly: KASAN: null-ptr-deref in range [0x0000000000000120-0x0000000000000127] CPU: 7 UID: 0 PID: 56 Comm: kworker/7:0 Not tainted 6.14.0-rc1+ Workqueue: vsock-loopback vsock_loopback_work RIP: 0010:vsock_read_skb+0x4b/0x90 Call Trace: sk_psock_verdict_data_ready+0xa4/0x2e0 virtio_transport_recv_pkt+0x1ca8/0x2acc vsock_loopback_work+0x27d/0x3f0 process_one_work+0x846/0x1420	cc9a7832ede53ade1ba9991f0e27314caa4029d8	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker_thread+0x5b3/0xf80 kthread+0x35a/0x700 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x1a/0x30 For connectible sockets, instead of relying solely on the state of vsk->transport, tell sockmap to only allow those representing established connections. This aligns with the behaviour for AF_INET and AF_UNIX. **CVE ID: CVE-2025-21854**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: acct: perform last write from workqueue In [1] it was reported that the acct(2) system call can be used to trigger NULL deref in cases where it is set to write to a file that triggers an internal lookup. This can e.g., happen when pointing acc(2) to /sys/power/resume. At the point the where the write to this file happens the calling task has already exited and called exit_fs(). A lookup will thus trigger a NULL-deref when accessing current->fs. Reorganize the code so that the the final write happens from the workqueue but with the caller's credentials. This preserves the	https://git.kernel.org/stable/c/56d5f3eba3f5de0efdd556de4ef381e109b973a9, https://git.kernel.org/stable/c/5a59ced8ffc71973d42c82484a719c8f6ac8f7f7, https://git.kernel.org/stable/c/5c928e14a2ccd99462f2351ead627b58075bb736	O-LIN-LINU-180325/2479

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(strange) permission model and has almost no regression risk. This api should stop to exist though. **CVE ID: CVE-2025-21846**		
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: avoid holding freeze_mutex during mmap operation We use map->freeze_mutex to prevent races between map_freeze() and memory mapping BPF map contents with writable permissions. The way we naively do this means we'll hold freeze_mutex for entire duration of all the mm and VMA manipulations, which is completely unnecessary. This can potentially also lead to deadlocks, as reported by syzbot in [0]. So, instead, hold freeze_mutex only during writeability checks, bump (proactively) "write active" count for the map, unlock the mutex and proceed with mmap logic. And only if something went wrong during mmap logic, then undo that "write active" counter increment. [0] https://lore.kernel.org/bpf/678dcbc9.050a0220.303755.0066.GAE@google.com/ **CVE ID: CVE-2025-21853**	https://git.kernel.org/stable/c/271e49f8a58edba65bc2b1250a0abaa98c4bfdbe, https://git.kernel.org/stable/c/29cfda62ab4d92ab94123813db49ab76c1e61b29, https://git.kernel.org/stable/c/bc27c52eea189e8f7492d40739b7746d67b65beb	O-LIN-LINU-180325/2480

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net: Add rx_skb of kfree_skb to raw_tp_null_args[]. Yan Zhai reported a BPF prog could trigger a null-ptr-deref [0] in trace_kfree_skb if the prog does not check if rx_sk is NULL. Commit c53795d48ee8 ("net: add rx_sk to trace_kfree_skb") added rx_sk to trace_kfree_skb, but rx_sk is optional and could be NULL. Let's add kfree_skb to raw_tp_null_args[] to let the BPF verifier validate such a prog and prevent the issue. Now we fail to load such a prog: libbpf: prog 'drop': -- BEGIN PROG LOAD LOG -- 0: R1=ctx() R10=fp0 ; int BPF_PROG(drop, struct sk_buff *skb, void *location, @ kfree_skb_sk_null.bpf.c:21 0: (79) r3 = *(u64 *)(r1 +24) func 'kfree_skb' arg3 has btf_id 5253 type STRUCT 'sock' 1: R1=ctx() R3_w=trusted_ptr_or_null_sock(id=1) ; bpf_printk("sk: %d, %d\n", sk, sk->__sk_common.skc_family); @ kfree_skb_sk_null.bpf.c:24 1: (69) r4 = *(u16 *)(r3 +16)	https://git.kernel.org/stable/c/4dba79c1e7aad6620bbb707b6c4459380fd90860, https://git.kernel.org/stable/c/5da7e15fb5a12e78de974d8908f348e279922ce9, https://git.kernel.org/stable/c/f579afacd0a66971fc8481f30d2d377e230a8342	O-LIN-LINU-180325/2481

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R3 invalid mem access 'trusted_ptr_or_null_' processed 2 insns (limit 1000000) max_states_per_insn 0 total_states 0 peak_states 0 mark_read 0 -- END PROG LOAD LOG -- Note this fix requires commit 838a10bd2ebf ("bpf: Augment raw_tp arguments with PTR_MAYBE_NULL"). [0]: BUG: kernel NULL pointer dereference, address: 0000000000000010 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 0 P4D 0 PREEMPT SMP RIP: 0010:bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d Call Trace: <TASK> ? __die+0x1f/0x60 ? page_fault_oops+0x148/0x420 ? search_bpf_extables+0x5b/0x70 ? fixup_exception+0x27/0x2c0 ? exc_page_fault+0x75/0x170 ? asm_exc_page_fault+0x22/0x30 ? bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d bpf_trace_run4+0x68/0xd0 ? unix_stream_connect+0x1f4/0x6f0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk_skb_reason_drop+0x90/0x120 unix_stream_connect+0x1f4/0x6f0 __sys_connect+0x7f/0xb0 __x64_sys_connect+0x14/0x20 do_syscall_64+0x47/0xc30 entry_SYSCALL_64_after_hwframe+0x4b/0x53 **CVE ID: CVE-2025-21852**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: stream-ipc: Check for cstream nullity in sof_ipc_msg_data() The nullity of sps->cstream should be checked similarly as it is done in sof_set_stream_data_offset() function. Assuming that it is not NULL if sps->stream is NULL is incorrect and can lead to NULL pointer dereference. **CVE ID: CVE-2025-21847**	https://git.kernel.org/stable/c/2b3878baf90918a361a3dfd3513025100b1b40b6, https://git.kernel.org/stable/c/62ab1ae5511c59b5f0bf550136ff321331adca9f, https://git.kernel.org/stable/c/6c18f5eb2043ebf4674c08a9690218dc818a11ab	O-LIN-LINU-180325/2482
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: bpf: Add check for nfp_app_ctrl_msg_alloc() Add check for the return value of nfp_app_ctrl_msg_alloc() in nfp_bpf_cmsg_alloc() to prevent null pointer dereference. **CVE ID: CVE-2025-21848**	https://git.kernel.org/stable/c/1358d8e07afdf21d49ca6f00c56048442977e00a, https://git.kernel.org/stable/c/29ccb1e4040da6ff02b7e64efaa2f8e6bf06020d, https://git.kernel.org/stable/c/878e7b11736e0	O-LIN-LINU-180325/2483

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				62514e58f3b445ff343e6705537	
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: fix error handling causing NULL dereference tcf_exts_miss_cookie_base_alloc() calls xa_alloc_cyclic() which can return 1 if the allocation succeeded after wrapping. This was treated as an error, with value 1 returned to caller tcf_exts_init_ex() which sets exts->actions to NULL and returns 1 to caller fl_change(). fl_change() treats err == 1 as success, calling tcf_exts_validate_ex() which calls tcf_action_init() with exts->actions as argument, where it is dereferenced. Example trace: BUG: kernel NULL pointer dereference, address: 0000000000000000 CPU: 114 PID: 16151 Comm: handler114 Kdump: loaded Not tainted 5.14.0-503.16.1.el9_5.x86_64 #1 RIP: 0010:tcf_action_init+0x1f8/0x2c0 Call Trace: tcf_action_init+0x1f8/0x2c0 tcf_exts_validate_ex+0x175/0x190 fl_change+0x537/0x1120 [cls_flower]	https://git.kernel.org/stable/c/071ed42cff4fcdd89025d966d48eabef59913bf2, https://git.kernel.org/stable/c/3c74b5787caf59bb1e9c5fe0a3600643a71eb1e8a, https://git.kernel.org/stable/c/3e4c56cf41876ef2a82f0877fe2a67648f8632b8	O-LIN-LINU-180325/2484

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21857		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Use spin_lock_irqsave() in interruptible context spin_lock/unlock() functions used in interrupt contexts could result in a deadlock, as seen in GitLab issue #13399, which occurs when interrupt comes in while holding a lock. Try to remedy the problem by saving irq state before spin lock acquisition. v2: add irqs' state save/restore calls to all locks/unlocks in signal_irq_work() execution (Maciej) v3: use with spin_lock_irqsave() in guc_lrc_desc_unpin() instead of other lock/unlock calls and add Fixes and Cc tags (Tvrtko); change title and commit message (cherry picked from commit c088387ddd6482b40f21ccf23db1125e8fa4af7e) **CVE ID: CVE-2025-21849**	https://git.kernel.org/stable/c/2bf1f4c129db7a10920655b000f0292f1ee509c2, https://git.kernel.org/stable/c/47ae46ac5407646420e06b78e0dad331e56a4bb4, https://git.kernel.org/stable/c/e49477f7f78598295551d486ecc7f020d796432e	O-LIN-LINU-180325/2485
Loop with Unreachable Exit Condition ('Infinite Loop')	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nvmet: Fix crash when a namespace is disabled	https://git.kernel.org/stable/c/4082326807072b71496501b6a0c55ffe8d5092a5,	O-LIN-LINU-180325/2486

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 namespace percpu counter protects pending I/O, and we can only safely diable the namespace once the counter drop to zero. Otherwise we end up with a crash when running blktests/nvme/058 (eg for loop transport): [2352.930426] [T53909] Oops: general protection fault, probably for non-canonical address 0xdffffc0000000005: 0000 [#1] PREEMPT SMP KASAN PTI [2352.930431] [T53909] KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] [2352.930434] [T53909] CPU: 3 UID: 0 PID: 53909 Comm: kworker/u16:5 Tainted: G W 6.13.0-rc6 #232 [2352.930438] [T53909] Tainted: [W]=WARN [2352.930440] [T53909] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-3.fc41 04/01/2014 [2352.930443] [T53909] Workqueue: nvmet-wq nvme_loop_execute_work [nvme_loop] [2352.930449] [T53909] RIP: 0010:blkcg_set_ioprio+0x44/0x180 as the queue is already torn down when calling submit_bio(); So we need to init the percpu counter in nvmet_ns_enable(), and	https://git.kernel.org/stable/c/cc0607594f6813342b27c752c6fb6f6eb9980cb5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wait for it to drop to zero in nvmet_ns_disable() to avoid having I/O pending after the namespace has been disabled. **CVE ID: CVE-2025-21850**		
Improper Locking	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix softlockup in arena_map_free on 64k page kernel On an aarch64 kernel with CONFIG_PAGE_SIZE_64KB=y, arena_htab tests cause a segmentation fault and soft lockup. The same failure is not observed with 4k pages on aarch64. It turns out arena_map_free() is calling apply_to_existing_page_range() with the address returned by bpf_arena_get_kern_vm_start(). If this address is not page-aligned the code ends up calling apply_to_pte_range() with that unaligned address causing soft lockup. Fix it by round up GUARD_SZ to PAGE_SIZE << 1 so that the division by 2 in bpf_arena_get_kern_vm_start() returns a page-aligned value. **CVE ID: CVE-2025-21851**	https://git.kernel.org/stable/c/517e8a7835e8cfb398a0aeb0133de50e31cae32b, https://git.kernel.org/stable/c/787d556a3de447e70964a4bdeba9196f62a62b1e, https://git.kernel.org/stable/c/c1f3f3892d4526f18aaeffdb6068ce861e793ee3	O-LIN-LINU-180325/2487
N/A	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/63895d20d63b4	O-LIN-LINU-180325/2488

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			mm/zswap: fix inconsistency when zswap_store_page() fails
			
			Commit b7c0ccdfbafd ("mm: zswap: support large folios in zswap_store()") skips charging any zswap entries when it failed to zswap the entire folio.
			
			However, when some base pages are zswapped but it failed to zswap the entire folio, the zswap operation is rolled back. When freeing zswap entries for those pages, zswap_entry_free() uncharges the zswap entries that were not previously charged, causing zswap charging to become inconsistent.
			
			This inconsistency triggers two warnings with following steps:
			# On a machine with 64GiB of RAM and 36GiB of zswap
			$ stress-ng --bigheap 2 # wait until the OOM-killer kills stress-ng
			$ sudo reboot
			
			The two warnings are:
			in mm/memcontrol.c:163, function obj_cgroup_release():
			
			WARN_ON_ONCE(nr_bytes & (PAGE_SIZE - 1));
			
			in mm/page_counter.c:60, function page_counter_cancel():
			if (WARN_ONCE(new < 0, "page_counter underflow: %ld nr_pages=%lu\n", new, nr_pages))
				46f5049a963983489319c2ea3e2, https://git.kernel.org/stable/c/a3652f5552b20903315612da487a7be2b95394d5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			zswap_stored_pages also becomes inconsistent in the same way. As suggested by Kanchana, increment zswap_stored_pages and charge zswap entries within zswap_store_page() when it succeeds. This way, zswap_entry_free() will decrement the counter and uncharge the entries when it failed to zswap the entire folio. While this could potentially be optimized by batching objcg charging and incrementing the counter, let's focus on fixing the bug this time and leave the optimization for later after some evaluation. After resolving the inconsistency, the warnings disappear. [42.hyeyoo@gmail.com: refactor zswap_store_page()] Link: https://lkml.kernel.org/r/20250131082037.2426-1-42.hyeyoo@gmail.com **CVE ID: CVE-2025-21860**		
Affected Version(s): 6.9					
Improper Locking	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix softlockup in arena_map_free on 64k page kernel On an aarch64 kernel with CONFIG_PAGE_SIZE_64KB=y,	https://git.kernel.org/stable/c/517e8a7835e8cfb398a0aeb0133de50e31cae32b, https://git.kernel.org/stable/c/787d556a3de447e70964a4bdeba9196f62a62b1e,	O-LIN-LINU-180325/2489

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arena_htab tests cause a segmentation fault and soft lockup. The same failure is not observed with 4k pages on aarch64. It turns out arena_map_free() is calling apply_to_existing_page_range() with the address returned by bpf_arena_get_kern_vm_start(). If this address is not page-aligned the code ends up calling apply_to_pte_range() with that unaligned address causing soft lockup. Fix it by round up GUARD_SZ to PAGE_SIZE << 1 so that the division by 2 in bpf_arena_get_kern_vm_start() returns a page-aligned value. **CVE ID: CVE-2025-21851**	https://git.kernel.org/stable/c/c1f3f3892d4526f18aaeffdb6068ce861e793ee3	
Affected Version(s): From (including) 2.6.12 Up to (excluding) 6.1.130					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: acct: perform last write from workqueue In [1] it was reported that the acct(2) system call can be used to trigger NULL deref in cases where it is set to write to a file that triggers an internal lookup. This can e.g., happen when pointing acct(2) to /sys/power/resume. At the point the where the write to this file happens the calling task has already exited and called	https://git.kernel.org/stable/c/56d5f3eba3f5de0efdd556de4ef381e109b973a9, https://git.kernel.org/stable/c/5a59ced8ffc71973d42c82484a719c8f6ac8f7f7, https://git.kernel.org/stable/c/5c928e14a2ccd99462f2351ead627b58075bb736	O-LIN-LINU-180325/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exit_fs(). A lookup will thus trigger a NULL-deref when accessing current->fs. Reorganize the code so that the the final write happens from the workqueue but with the caller's credentials. This preserves the (strange) permission model and has almost no regression risk. This api should stop to exist though. **CVE ID: CVE-2025-21846**		
Affected Version(s): From (including) 2.6.30 Up to (excluding) 6.1.130					
Use of Uninitialized Resource	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix incorrect initialization order Syzkaller reports the following bug: BUG: spinlock bad magic on CPU#1, syz-executor.0/7995 lock: 0xffff88805303f3e0, .magic: 00000000, .owner: <none>/-1, .owner_cpu: 0 CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted: G E 5.10.209+ #1 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x119/0x179 lib/dump_stack.c:118 debug_spin_lock_before kernel/locking/spinlock_de	https://git.kernel.org/stable/c/07b598c0e6f06a0f254c88dafb4ad50f8a8c6eea, https://git.kernel.org/stable/c/0efa6c42f81c60d8f72ba7f5ed8d4fec8c526282, https://git.kernel.org/stable/c/219a47d0e6195bd202f22855e35f25bd15bc4d58	O-LIN-LINU-180325/2491

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bug.c:83 [inline] do_raw_spin_lock+0x1f6/0x270 kernel/locking/spinlock_debug.c:112 __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:117 [inline] _raw_spin_lock_irqsave+0x50/0x70 kernel/locking/spinlock.c:159 reset_per_cpu_data+0xe6/0x240 [drop_monitor] net_dm_cmd_trace+0x43d/0x17a0 [drop_monitor] genl_family_rcv_msg_doit+0x22f/0x330 net/netlink/genetlink.c:739 genl_family_rcv_msg net/netlink/genetlink.c:783 [inline] genl_rcv_msg+0x341/0x5a0 net/netlink/genetlink.c:800 netlink_rcv_skb+0x14d/0x440 net/netlink/af_netlink.c:2497 genl_rcv+0x29/0x40 net/netlink/genetlink.c:811 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x54b/0x800 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x914/0xe00 net/netlink/af_netlink.c:1916 sock_sendmsg_nosec net/socket.c:651 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sock_sendmsg+0x157/0x190 net/socket.c:663 ____sys_sendmsg+0x712/0x870 net/socket.c:2378 ___sys_sendmsg+0xf8/0x170 net/socket.c:2432 __sys_sendmsg+0xea/0x1b0 net/socket.c:2461 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x62/0xc7 RIP: 0033:0x7f3f9815aee9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3f972bf0c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f3f9826d050 RCX: 00007f3f9815aee9 RDX: 0000000020000000 RSI: 0000000020001300 RDI: 0000000000000007 RBP: 00007f3f981b63bd R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f3f9826d050 R15: 00007ffe01ee6768 If drop_monitor is built as a kernel module, syzkaller may have time to send a netlink NET_DM_CMD_START		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			message during the module loading. This will call the net_dm_monitor_start() function that uses a spinlock that has not yet been initialized. To fix this, let's place resource initialization above the registration of a generic netlink family. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with Syzkaller. **CVE ID: CVE-2025-21862**		
Affected Version(s): From (including) 3.2 Up to (excluding) 6.1.130					
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: f_midi: f_midi_complete to call queue_work When using USB MIDI, a lock is attempted to be acquired twice through a re-entrant call to f_midi_transmit, causing a deadlock. Fix it by using queue_work() to schedule the inner f_midi_transmit() via a high priority work queue from the completion handler. **CVE ID: CVE-2025-21859**	https://git.kernel.org/stable/c/1f10923404705a94891e612dff3b75e828a78368, https://git.kernel.org/stable/c/24a942610ee9bafb2692a456ae850c5b2e409b05, https://git.kernel.org/stable/c/4ab37fcb42832cdd3e9d5e50653285ca84d6686f	O-LIN-LINU-180325/2492
Affected Version(s): From (including) 4.13 Up to (excluding) 6.1.130					
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/code-patching: Fix KASAN hit by not flagging	https://git.kernel.org/stable/c/2d542f13d26344e3452eee77613026ce9b653065,	O-LIN-LINU-180325/2493

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			text patching area as VM_ALLOC Erhard reported the following KASAN hit while booting his PowerMac G4 with a KASAN-enabled kernel 6.13-rc6: BUG: KASAN: vmalloc-out-of-bounds in copy_to_kernel_nofault+0xd8/0x1c8 Write of size 8 at addr f1000000 by task chronyd/1293 CPU: 0 UID: 123 PID: 1293 Comm: chronyd Tainted: G W 6.13.0-rc6-PMacG4 #2 Tainted: [W]=WARN Hardware name: PowerMac3,6 7455 0x80010303 PowerMac Call Trace: [c2437590] [c1631a84] dump_stack_lvl+0x70/0x8c (unreliable) [c24375b0] [c0504998] print_report+0xdc/0x504 [c2437610] [c050475c] kasan_report+0xf8/0x108 [c2437690] [c0505a3c] kasan_check_range+0x24/0x18c [c24376a0] [c03fb5e4] copy_to_kernel_nofault+0xd8/0x1c8 [c24376c0] [c004c014] patch_instructions+0x15c/0x16c [c2437710] [c00731a8] bpf_arch_text_copy+0x60/0x7c [c2437730] [c0281168] bpf_jit_binary_pack_finalize+0x50/0xac [c2437750] [c0073cf4] bpf_int_jit_compile+0xb30/0xdec [c2437880] [c0280394]	https://git.kernel.org/stable/c/2e6c80423f201405fd65254e52decd21663896f3, https://git.kernel.org/stable/c/6847b3e40bb963e57b61d1cc6fe84cb37b9d3d4c	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf_prog_select_runtime+0x15c/0x478 [c24378d0] [c1263428] bpf_prepare_filter+0xbf8/0xc14 [c2437990] [c12677ec] bpf_prog_create_from_user+0x258/0x2b4 [c24379d0] [c027111c] do_seccomp+0x3dc/0x1890 [c2437ac0] [c001d8e0] system_call_exception+0x2dc/0x420 [c2437f30] [c00281ac] ret_from_syscall+0x0/0x2c --- interrupt: c00 at 0x5a1274 NIP: 005a1274 LR: 006a3b3c CTR: 005296c8 REGS: c2437f40 TRAP: 0c00 Tainted: G W (6.13.0-rc6-PMacG4) MSR: 0200f932 <VEC,EE,PR,FP,ME,IR,DR,RI> CR: 24004422 XER: 00000000 GPR00: 00000166 af8f3fa0 a7ee3540 00000001 00000000 013b6500 005a5858 0200f932 GPR08: 00000000 00001fe9 013d5fc8 005296c8 2822244c 00b2fcd8 00000000 af8f4b57 GPR16: 00000000 00000001 00000000 00000000 00000000 00000001 00000000 00000002 GPR24: 00afdbb0 00000000 00000000 00000000 006e0004 013ce060 006e7c1c 00000001 NIP [005a1274] 0x5a1274 LR [006a3b3c] 0x6a3b3c --- interrupt: c00 The buggy address belongs to the virtual mapping at		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[f1000000, f1002000) created by: text_area_cpu_up+0x20/0x190 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x76e30 flags: 0x80000000(zone=2) raw: 80000000 00000000 00000122 00000000 00000000 00000000 ffffffff 00000001 raw: 00000000 page dumped because: kasan: bad access detected Memory state around the buggy address: f0ffff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0ffff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >f1000000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ f1000080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f1000100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ========== f8 corresponds to KASAN_VMALLOC_INVALID which means the area is not initialised hence not supposed to be used yet. Powerpc text patching infrastructure allocates a virtual memory area		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using get_vm_area() and flags it as VM_ALLOC. But that flag is meant to be used for vmalloc() and vmalloc() allocated memory is not supposed to be used before a call to __vmalloc_node_range() which is never called for that area. That went undetected until commit e4137f08816b ("mm, kasan, kmsan: instrument copy_from/to_kernel_nofault") The area allocated by text_area_cpu_up() is not vmalloc memory, it is mapped directly on demand when needed by map_kernel_page(). There is no VM flag corresponding to such usage, so just pass no flag. That way the area will be unpoisonned and usable immediately. **CVE ID: CVE-2025-21866**		
Affected Version(s): From (including) 4.14 Up to (excluding) 6.12.17					
Use After Free	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/migrate_device: don't add folio to be freed to LRU in migrate_device_finalize() If migration succeeded, we called folio_migrate_flags()->mem_cgroup_migrate() to migrate the memcg from the old to the new folio. This will set memcg_data of the old folio to 0.	https://git.kernel.org/stable/c/069dd21ea8262204f94737878389c2815a054a9e, https://git.kernel.org/stable/c/3f9240d59e9a95d19f06120bfd1d0e681c6c0ac7, https://git.kernel.org/stable/c/41cddf83d8b00f29fd105e7a0777366edc69a5cf	O-LIN-LINU-180325/2494

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Similarly, if migration failed, memcg_data of the dst folio is left unset. If we call folio_putback_lru() on such folios (memcg_data == 0), we will add the folio to be freed to the LRU, making memcg code unhappy. Running the hmm selftests: # ./hmm-tests ... # RUN hmm.hmm_device_private.migrate ... [102.078007][T14893] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x7ff27d200 pfn:0x13cc00 [102.079974][T14893] anon flags: 0x17ff00000020018(uptodate|dirty|swapbacked|node=0|zone=2|lastcpupid=0x7ff) [102.082037][T14893] raw: 017ff00000020018 dead000000000100 dead000000000122 ffff8881353896c9 [102.083687][T14893] raw: 00000007ff27d200 0000000000000000 00000001ffffffff 0000000000000000 [102.085331][T14893] page dumped because: VM_WARN_ON_ONCE_FOLIO(!memcg && !mem_cgroup_disabled()) [102.087230][T14893] ------------[cut here]------------ [102.088279][T14893] WARNING: CPU: 0 PID: 14893 at ./include/linux/memcontrol.h:726 folio_lruvec_lock_irqsave+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
			x10e/0x170 [102.090478][T14893] Modules linked in: [102.091244][T14893] CPU: 0 UID: 0 PID: 14893 Comm: hmm-tests Not tainted 6.13.0-09623-g6c216bc522fd #151 [102.093089][T14893] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 [102.094848][T14893] RIP: 0010:folio_lruvec_lock_irqsave+0x10e/0x170 [102.096104][T14893] Code: ... [102.099908][T14893] RSP: 0018:ffffc900236c37b0 EFLAGS: 00010293 [102.101152][T14893] RAX: 0000000000000000 RBX: ffffea0004f30000 RCX: ffffffff8183f426 [102.102684][T14893] RDX: ffff8881063cb880 RSI: ffffffff81b8117f RDI: ffff8881063cb880 [102.104227][T14893] RBP: 0000000000000000 R08: 0000000000000005 R09: 0000000000000000 [102.105757][T14893] R10: 0000000000000001 R11: 0000000000000002 R12: ffffc900236c37d8 [102.107296][T14893] R13: ffff888277a2bcb0 R14: 000000000000001f R15: 0000000000000000 [102.108830][T14893] FS: 00007ff27dbdd740(0000) GS:ffff888277a00000(0000) knlGS:0000000000000000 [102.110643][T14893] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[102.111924][T14893] CR2: 00007ff27d400000 CR3: 000000010866e000 CR4: 0000000000750ef0 [102.113478][T14893] PKRU: 55555554 [102.114172][T14893] Call Trace: [102.114805][T14893] <TASK> [102.115397][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.116547][T14893] ? __warn.cold+0x110/0x210 [102.117461][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.118667][T14893] ? report_bug+0x1b9/0x320 [102.119571][T14893] ? handle_bug+0x54/0x90 [102.120494][T14893] ? exc_invalid_op+0x17/0x50 [102.121433][T14893] ? asm_exc_invalid_op+0x1a/0x20 [102.122435][T14893] ? __wake_up_klogd.part.0+0x76/0xd0 [102.123506][T14893] ? dump_page+0x4f/0x60 [102.124352][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.125500][T14893] folio_batch_move_lru+0xd4/0x200 [102.126577][T14893] ? __pfx_lru_add+0x10/0x10 [102.127505][T14893] __folio_batch_add_and_move+0x391/0x720 [102.128633][T14893] ? __pfx_lru_add+0x10/0x10 [102.129550][T14893] folio_putback_lru+0x16/0x80 [102.130564][T14893] migrate_device_finalize+0x9b/0x530 [102.131640][T14893]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dmirror_migrate_to_device.constprop.0+0x7c5/0xad0 [102.133047][T14893] dmirror_fops_unlocked_ioctl+0x89b/0xc80 Likely, nothing else goes wrong: putting the last folio reference will remove the folio from the LRU again. So besides memcg complaining, adding the folio to be freed to the LRU is just an unnecessary step. The new flow resembles what we have in migrate_folio_move(): add the dst to the lru, rem ---truncated--- **CVE ID: CVE-2025-21861**		
Affected Version(s): From (including) 4.16 Up to (excluding) 6.1.130					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: bpf: Add check for nfp_app_ctrl_msg_alloc() Add check for the return value of nfp_app_ctrl_msg_alloc() in nfp_bpf_cmsg_alloc() to prevent null pointer dereference. **CVE ID: CVE-2025-21848**	https://git.kernel.org/stable/c/1358d8e07afdf21d49ca6f00c56048442977e00a, https://git.kernel.org/stable/c/29ccb1e4040da6ff02b7e64efaa2f8e6bf06020d, https://git.kernel.org/stable/c/878e7b11736e062514e58f3b445ff343e6705537	O-LIN-LINU-180325/2495
Affected Version(s): From (including) 4.2 Up to (excluding) 6.1.130					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller reported a use-	https://git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf, https://git.kernel.org/stable/c/5a0538ac68268	O-LIN-LINU-180325/2496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free in geneve_find_dev() [0] without repro. geneve_configure() links struct geneve_dev.next to net_generic(net, geneve_net_id)->geneve_list. The net here could differ from dev_net(dev) if IFLA_NET_NS_PID, IFLA_NET_NS_FD, or IFLA_TARGET_NETNSID is set. When dev_net(dev) is dismantled, geneve_exit_batch_rtnl() finally calls unregister_netdevice_queue() for each dev in the netns, and later the dev is freed. However, its geneve_dev.next is still linked to the backend UDP socket netns. Then, use-after-free will occur when another geneve dev is created in the netns. Let's call geneve_dellink() instead in geneve_destroy_tunnels(). [0]: BUG: KASAN: slab-use-after-free in geneve_find_dev drivers/net/geneve.c:1295 [inline] BUG: KASAN: slab-use-after-free in geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 Read of size 2 at addr ffff000054d6ee24 by task	07d6919f6aecbb8996c2865af2c, https://git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syz.1.4029/13441 CPU: 1 UID: 0 PID: 13441 Comm: syz.1.4029 Not tainted 6.13.0-g0ad9617c78ac #24 dc35ca22c79fb82e8e7bc5c9c9adafea898b1e3d Hardware name: linux,dummy-virt (DT) Call trace: show_stack+0x38/0x50 arch/arm64/kernel/stacktrace.c:466 (C) __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xbc/0x108 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x16c/0x6f0 mm/kasan/report.c:489 kasan_report+0xc0/0x120 mm/kasan/report.c:602 __asan_report_load2_noabort+0x20/0x30 mm/kasan/report_generic.c:379 geneve_find_dev drivers/net/geneve.c:1295 [inline] geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 geneve_newlink+0xb8/0x128 drivers/net/geneve.c:1634 rtnl_newlink_create+0x23c/0x868 net/core/rtnetlink.c:3795 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x618/0x838 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x5fc/0x8b0 net/netlink/af_netlink.c:1892 sock_sendmsg_nosec net/socket.c:713 [inline] __sock_sendmsg net/socket.c:728 [inline] ___sys_sendmsg+0x410/0x6f8 net/socket.c:2568 __sys_sendmsg+0x178/0x1d8 net/socket.c:2622 __sys_sendmsg net/socket.c:2654 [inline] __do_sys_sendmsg net/socket.c:2659 [inline] __se_sys_sendmsg net/socket.c:2657 [inline] __arm64_sys_sendmsg+0x12c/0x1c8 net/socket.c:2657 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x90/0x278 arch/arm64/kernel/syscall.c:49		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0_svc_common+0x13c/0x250 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x54/0x70 arch/arm64/kernel/syscall.c:151 el0_svc+0x4c/0xa8 arch/arm64/kernel/entry-common.c:744 el0t_64_sync_handler+0x78/0x108 arch/arm64/kernel/entry-common.c:762 el0t_64_sync+0x198/0x1a0 arch/arm64/kernel/entry.S:600 Allocated by task 13247: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x68 mm/kasan/common.c:68 kasan_save_alloc_info+0x44/0x58 mm/kasan/generic.c:568 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x84/0xa0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4298 [inline] __kmalloc_node_noprof+0x2a0/0x560 mm/slub.c:4304 __kvmalloc_node_noprof+0x9c/0x230 mm/util.c:645 alloc_netdev_mqs+0xb8/0x11a0 net/core/dev.c:11470		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rtnl_create_link+0x2b8/0xb50 net/core/rtnetlink.c:3604 rtnl_newlink_create+0x19c/0x868 net/core/rtnetlink.c:3780 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_n ---truncated--- **CVE ID: CVE-2025-21858**		
Affected Version(s): From (including) 4.5 Up to (excluding) 6.1.130					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Don't reference skb after sending to VIOS Previously, after successfully flushing the xmit buffer to VIOS, the tx_bytes stat was incremented by the length of the skb. It is invalid to access the skb memory after sending the buffer to the VIOS because, at any point after sending, the VIOS	https://git.kernel.org/stable/c/093b0e5c90592773863f300b908b741622eef597, https://git.kernel.org/stable/c/25dddd01dcc8ef3acff964dbb32eeb0d89f098e9, https://git.kernel.org/stable/c/501ac6a7e21b82e05207c6b4449812d82820f306	O-LIN-LINU-180325/2497

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 trigger an interrupt to free this memory. A race between reading skb->len and freeing the skb is possible (especially during LPM) and will result in use-after-free: ========== ========== ========== === BUG: KASAN: slab-use-after-free in ibmvnic_xmit+0x75c/0x1808 [ibmvnic] Read of size 4 at addr c00000024eb48a70 by task hxecom/14495 <...> Call Trace: [c000000118f66cf0] [c0000000018cba6c] dump_stack_lvl+0x84/0xe8 (unreliable) [c000000118f66d20] [c0000000006f0080] print_report+0x1a8/0x7f0 [c000000118f66df0] [c0000000006f08f0] kasan_report+0x128/0x1f8 [c000000118f66f00] [c0000000006f2868] __asan_load4+0xac/0xe0 [c000000118f66f20] [c0080000046eac84] ibmvnic_xmit+0x75c/0x1808 [ibmvnic] [c000000118f67340] [c0000000014be168] dev_hard_start_xmit+0x150/0x358 <...> Freed by task 0: kasan_save_stack+0x34/0x68 kasan_save_track+0x2c/0x50		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kasan_save_free_info+0x64/0x108 __kasan_mempool_poison_object+0x148/0x2d4 napi_skb_cache_put+0x5c/0x194 net_tx_action+0x154/0x5b8 handle_softirqs+0x20c/0x60c do_softirq_own_stack+0x6c/0x88 <...> The buggy address belongs to the object at c00000024eb48a00 which belongs to the cache skbuff_head_cache of size 224 ========== ========== ========== === **CVE ID: CVE-2025-21855**		
Affected Version(s): From (including) 5.0 Up to (excluding) 6.12.17					
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double accounting race when btrfs_run_delalloc_range() failed [BUG] When running btrfs with block size (4K) smaller than page size (64K, aarch64), there is a very high chance to crash the kernel at generic/750, with the following messages: (before the call traces, there are 3 extra debug messages added)	https://git.kernel.org/stable/c/0283ee1912c8e243c931f4ee5b3672e954fe0384, https://git.kernel.org/stable/c/21333148b5c9e52f41fafcedec3810b56a5e0e40, https://git.kernel.org/stable/c/72dad8e377afa50435940adfb697e070d3556670	O-LIN-LINU-180325/2498

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			BTRFS warning (device dm-3): read-write for sector size 4096 with page size 65536 is experimental BTRFS info (device dm-3): checking UUID tree hrtimer: interrupt took 5451385 ns BTRFS error (device dm-3): cow_file_range failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): run_delalloc_nocow failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): failed to run delalloc range, root=4957 ino=257 folio=1572864 submit_bitmap=8-15 start=1605632 len=69632: -28 ------------[cut here]------------ WARNING: CPU: 2 PID: 3020984 at ordered-data.c:360 can_finish_ordered_extent+0x370/0x3b8 [btrfs] CPU: 2 UID: 0 PID: 3020984 Comm: kworker/u24:1 Tainted: G OE 6.13.0-rc1-custom+ #89 Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: events_unbound btrfs_async_reclaim_data_space [btrfs] pc : can_finish_ordered_extent+0x370/0x3b8 [btrfs] lr : can_finish_ordered_extent+		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x1ec/0x3b8 [btrfs] Call trace: can_finish_ordered_extent+0x370/0x3b8 [btrfs] (P) can_finish_ordered_extent+0x1ec/0x3b8 [btrfs] (L) btrfs_mark_ordered_io_finished+0x130/0x2b8 [btrfs] extent_writepage+0x10c/0x3b8 [btrfs] extent_write_cache_pages+0x21c/0x4e8 [btrfs] btrfs_writepages+0x94/0x160 [btrfs] do_writepages+0x74/0x190 filemap_fdatawrite_wbc+0x74/0xa0 start_delalloc_inodes+0x17c/0x3b0 [btrfs] btrfs_start_delalloc_roots+0x17c/0x288 [btrfs] shrink_delalloc+0x11c/0x280 [btrfs] flush_space+0x288/0x328 [btrfs] btrfs_async_reclaim_data_space+0x180/0x228 [btrfs] process_one_work+0x228/0x680 worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- BTRFS critical (device dm-3): bad ordered extent accounting, root=4957		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ino=257 OE offset=1605632 OE len=16384 to_dec=16384 left=0 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1622016 OE len=12288 to_dec=12288 left=0 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1634304 OE len=8192 to_dec=4096 left=0 CPU: 1 UID: 0 PID: 3286940 Comm: kworker/u24:3 Tainted: G W OE 6.13.0-rc1-custom+ #89 Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: btrfs_work_helper [btrfs] (btrfs-endio-write) pstate: 404000c5 (nZcv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : process_one_work+0x110/0x680 lr : worker_thread+0x1bc/0x360 Call trace: process_one_work+0x110/0x680 (P) worker_thread+0x1bc/0x360 (L) worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 Code: f84086a1 f9000fe1 53041c21 b9003361		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(f9400661) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception SMP: stopping secondary CPUs SMP: failed to stop secondary CPUs 2-3 Dumping ftrace buffer: (ftrace buffer empty) Kernel Offset: 0x275bb9540000 from 0xffff800080000000 PHYS_OFFSET: 0xffff8fbba0000000 CPU features: 0x100,00000070,00801250,8201720b [CAUSE] The above warning is triggered immediately after the delalloc range failure, this happens in the following sequence: - Range [1568K, 1636K) is dirty 1536K 1568K 1600K 1636K 1664K | |/////////\////////| | Where 1536K, 1600K and 1664K are page boundaries (64K page size) - Enter extent_writepage() for page 1536K - Enter run_delalloc_nocow() with locke ---truncated--- **CVE ID: CVE-2024-58089**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.68					
Concurrent Execution	02-Mar-2025	4.7	In the Linux kernel, the following vulnerability has	https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the params_lock mutex for the rest. When the stream is set up again by another thread between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same params_lock mutex with snd_pcm_oss_make_ready_locked() variant. **CVE ID: CVE-2022-49733**	4051324a6dafd7053c74c475e80b3ba10ae672b0, https://git.kernel.org/stable/c/723ac5ab2891b6c10dd6cc78ef5456af593490eb, https://git.kernel.org/stable/c/8015ef9e8a0ee5cecfd0cb6805834d007ab26f86	
Affected Version(s): From (including) 5.16 Up to (excluding) 5.19.9					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Mar-2025	4.7	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the	https://git.kernel.org/stable/c/4051324a6dafd7053c74c475e80b3ba10ae672b0, https://git.kernel.org/stable/c/723ac5ab2891b6c10dd6cc78ef5456af593490eb, https://git.kernel.org/stable/c/8015ef9e8a0ee5cecfd0cb6805834d007ab26f86	O-LIN-LINU-180325/2500

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			params_lock mutex for the rest. When the stream is set up again by another thread between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same params_lock mutex with snd_pcm_oss_make_ready_locked() variant. **CVE ID: CVE-2022-49733**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.121					
Improper Locking	12-Mar-2025	8.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid racy issue with session expire. **CVE ID: CVE-2024-58087**	https://git.kernel.org/stable/c/2107ab40629aeabbec369cf34b8cf0f288c3eb1b, https://git.kernel.org/stable/c/37a0e2b362b3150317fb6e2139de67b1e29ae5ff, https://git.kernel.org/stable/c/450a844c045ff0895d41b05a1cbe8febd1acfcfd	O-LIN-LINU-180325/2501
Affected Version(s): From (including) 5.19 Up to (excluding) 6.1.130					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop dst Xiumei reported hitting the WARN in xfrm6_tunnel_net_exit while running tests that boil down to:	https://git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9, https://git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491, https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2502

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			- create a pair of netns - run a basic TCP test over ipcomp6 - delete the pair of netns The xfrm_state found on spi_byaddr was not deleted at the time we delete the netns, because we still have a reference on it. This lingering reference comes from a secpath (which holds a ref on the xfrm_state), which is still attached to an skb. This skb is not leaked, it ends up on sk_receive_queue and then gets defer-free'd by skb_attempt_defer_free. The problem happens when we defer freeing an skb (push it on one CPU's defer_list), and don't flush that list before the netns is deleted. In that case, we still have a reference on the xfrm_state that we don't expect at this point. We already drop the skb's dst in the TCP receive path when it's no longer needed, so let's also drop the secpath. At this point, tcp_filter has already called into the LSM hooks that may require the secpath, so it should not be needed anymore. However, in some of those places, the MPTCP extension has just been attached to the skb, so we cannot simply drop all extensions. **CVE ID: CVE-2025-21864**	9b6412e6979f6f9e0632075f8f008937b5cd4efd	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 5.5 Up to (excluding) 5.10.148					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Mar-2025	4.7	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the params_lock mutex for the rest. When the stream is set up again by another thread between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same params_lock mutex with snd_pcm_oss_make_ready_locked() variant. **CVE ID: CVE-2022-49733**	https://git.kernel.org/stable/c/4051324a6dafd7053c74c475e80b3ba10ae672b0, https://git.kernel.org/stable/c/723ac5ab2891b6c10dd6cc78ef5456af593490eb, https://git.kernel.org/stable/c/8015ef9e8a0ee5cecfd0cb6805834d007ab26f86	O-LIN-LINU-180325/2503
Affected Version(s): From (including) 5.5 Up to (excluding) 6.6.80					
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: avoid holding freeze_mutex during mmap operation We use map->freeze_mutex to prevent races between map_freeze() and memory mapping BPF map	https://git.kernel.org/stable/c/271e49f8a58edba65bc2b1250a0abaa98c4bfdbe, https://git.kernel.org/stable/c/29cfda62ab4d92ab94123813db49ab76c1e61b29,	O-LIN-LINU-180325/2504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contents with writable permissions. The way we naively do this means we'll hold freeze_mutex for entire duration of all the mm and VMA manipulations, which is completely unnecessary. This can potentially also lead to deadlocks, as reported by syzbot in [0]. So, instead, hold freeze_mutex only during writeability checks, bump (proactively) "write active" count for the map, unlock the mutex and proceed with mmap logic. And only if something went wrong during mmap logic, then undo that "write active" counter increment. [0] https://lore.kernel.org/bpf/678dcbc9.050a0220.303755.0066.GAE@google.com/ **CVE ID: CVE-2025-21853**	https://git.kernel.org/stable/c/bc27c52eea189e8f7492d40739b7746d67b65beb	
Affected Version(s): From (including) 5.6 Up to (excluding) 6.6.80					
N/A	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: io_uring: prevent opcode speculation sqe->opcode is used for different tables, make sure we santitise it against speculations. **CVE ID: CVE-2025-21863**	https://git.kernel.org/stable/c/1e988c3fe1264708f4f92109203ac5b1d65de50b, https://git.kernel.org/stable/c/506b9b5e8c2d2a411ea8fe361333f5081c56d23a, https://git.kernel.org/stable/c/b9826e3b26ec031e9063f64a7c735449c43955e4	O-LIN-LINU-180325/2505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.1.127 Up to (excluding) 6.1.130					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl()	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2506

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue (). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack fffffe8040b4fbd0+0x7bd0/0x8000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[kworker/u8:7+netns 1804] R09: kasan shadow of process kstack ffffffe8040b4f990+0x7990/ 0x8000 [kworker/u8:7+netns 1804] R10: process kstack ffffffe8040b4f997+0x7997/ 0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_ core_dev_11127_8_1328_8_ S_4096_A_64_n_139+0xc08 /0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 ffffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] ffffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): From (including) 6.1.69 Up to (excluding) 6.1.130					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2507
Affected Version(s): From (including) 6.11 Up to (excluding) 6.12.17					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net: Add rx_skb of kfree_skb to raw_tp_null_args[]. Yan Zhai reported a BPF prog could trigger a null-ptr-deref [0] in trace_kfree_skb if the prog does not check if rx_sk is NULL. Commit c53795d48ee8 ("net: add rx_sk to trace_kfree_skb") added rx_sk to trace_kfree_skb, but rx_sk is optional and could be NULL. Let's add kfree_skb to raw_tp_null_args[] to let the BPF verifier	https://git.kernel.org/stable/c/4dba79c1e7aad6620bbb707b6c4459380fd90860, https://git.kernel.org/stable/c/5da7e15fb5a12e78de974d8908f348e279922ce9, https://git.kernel.org/stable/c/f579afacd0a66971fc8481f30d2d377e230a8342	O-LIN-LINU-180325/2508

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate such a prog and prevent the issue. Now we fail to load such a prog: libbpf: prog 'drop': -- BEGIN PROG LOAD LOG -- 0: R1=ctx() R10=fp0 ; int BPF_PROG(drop, struct sk_buff *skb, void *location, @ kfree_skb_sk_null.bpf.c:21 0: (79) r3 = *(u64 *)(r1 +24) func 'kfree_skb' arg3 has btf_id 5253 type STRUCT 'sock' 1: R1=ctx() R3_w=trusted_ptr_or_null_sock(id=1) ; bpf_printk("sk: %d, %d\n", sk, sk->__sk_common.skc_family); @ kfree_skb_sk_null.bpf.c:24 1: (69) r4 = *(u16 *)(r3 +16) R3 invalid mem access 'trusted_ptr_or_null_' processed 2 insns (limit 1000000) max_states_per_insn 0 total_states 0 peak_states 0 mark_read 0 -- END PROG LOAD LOG -- Note this fix requires commit 838a10bd2ebf ("bpf: Augment raw_tp arguments with PTR_MAYBE_NULL"). [0]: BUG: kernel NULL pointer dereference, address: 0000000000000010 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 0 P4D 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
			PREEMPT SMP RIP: 0010:bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d Call Trace: <TASK> ? __die+0x1f/0x60 ? page_fault_oops+0x148/0x420 ? search_bpf_extables+0x5b/0x70 ? fixup_exception+0x27/0x2c0 ? exc_page_fault+0x75/0x170 ? asm_exc_page_fault+0x22/0x30 ? bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d bpf_trace_run4+0x68/0xd0 ? unix_stream_connect+0x1f4/0x6f0 sk_skb_reason_drop+0x90/0x120 unix_stream_connect+0x1f4/0x6f0 __sys_connect+0x7f/0xb0 __x64_sys_connect+0x14/0x20 do_syscall_64+0x47/0xc30 entry_SYSCALL_64_after_hwframe+0x4b/0x53 **CVE ID: CVE-2025-21852**		
Affected Version(s): From (including) 6.12 Up to (excluding) 6.12.17					
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mtd: spi-nor: sst: Fix SST write failure	https://git.kernel.org/stable/c/539bd20352832b9244238a055eb169ccf1c41ff6, https://git.kern	O-LIN-LINU-180325/2509

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			'commit 18bcb4aa54ea ("mtd: spi-nor: sst: Factor out common write operation to `sst_nor_write_data()`")' introduced a bug where only one byte of data is written, regardless of the number of bytes passed to sst_nor_write_data(), causing a kernel crash during the write operation. Ensure the correct number of bytes are written as passed to sst_nor_write_data(). Call trace: [57.400180] ----------[cut here]---------- [57.404842] While writing 2 byte written 1 bytes [57.409493] WARNING: CPU: 0 PID: 737 at drivers/mtd/spi-nor/sst.c:187 sst_nor_write_data+0x6c/0x74 [57.418464] Modules linked in: [57.421517] CPU: 0 UID: 0 PID: 737 Comm: mtd_debug Not tainted 6.12.0-g5ad04afd91f9 #30 [57.429517] Hardware name: Xilinx Versal A2197 Processor board revA - x-prc-02 revA (DT) [57.437600] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [57.444557] pc : sst_nor_write_data+0x6c/0x74 [57.448911] lr : sst_nor_write_data+0x6c/0x74 [57.453264] sp : ffff80008232bb40 [57.456570] x29:	el.org/stable/c/9553391f32f8c43e12fc7c04e1035160b5ea20bf, https://git.kernel.org/stable/c/bb1accc7e0f688886f0c634f2e878b8ac4ee6a58	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff80008232bb40 x28: 0000000000010000 x27: 0000000000000001 [57.463708] x26: 000000000000ffff x25: 0000000000000000 x24: 0000000000000000 [57.470843] x23: 0000000000010000 x22: ffff80008232bbf0 x21: ffff000816230000 [57.477978] x20: ffff0008056c0080 x19: 0000000000000002 x18: 0000000000000006 [57.485112] x17: 0000000000000000 x16: 0000000000000000 x15: ffff80008232b580 [57.492246] x14: 0000000000000000 x13: ffff8000816d1530 x12: 00000000000004a4 [57.499380] x11: 000000000000018c x10: ffff8000816fd530 x9 : ffff8000816d1530 [57.506515] x8 : 00000000fffff7ff x7 : ffff8000816fd530 x6 : 0000000000000001 [57.513649] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [57.520782] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0008049b0000 [57.527916] Call trace: [57.530354] sst_nor_write_data+0x6c/0x74 [57.534361] sst_nor_write+0xb4/0x18c [57.538019] mtd_write_oob_std+0x7c/0x88 [57.541941] mtd_write_oob+0x70/0xbc [57.545511] mtd_write+0x68/0xa8		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[57.548733] mtdchar_write+0x10c/0x290 [57.552477] vfs_write+0xb4/0x3a8 [57.555791] ksys_write+0x74/0x10c [57.559189] __arm64_sys_write+0x1c/0x28 [57.563109] invoke_syscall+0x54/0x11c [57.566856] el0_svc_common.constprop.0+0xc0/0xe0 [57.571557] do_el0_svc+0x1c/0x28 [57.574868] el0_svc+0x30/0xcc [57.577921] el0t_64_sync_handler+0x120/0x12c [57.582276] el0t_64_sync+0x190/0x194 [57.585933] ---[end trace 0000000000000000]--- [pratyush@kernel.org: add Cc stable tag] **CVE ID: CVE-2025-21845**		
Affected Version(s): From (including) 6.12.11 Up to (excluding) 6.12.17					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl()	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2510

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue(). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: fffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack fffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack fffffe8040b4f990+0x7990/0x8000 [kworker/u8:7+netns 1804] R10: process kstack fffffe8040b4f997+0x7997/0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc08/0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 fffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): From (including) 6.13 Up to (excluding) 6.13.4					
Use of Uninitialized Resource	07-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: avoid garbage value in panthor_ioctl_dev_query() 'priorities_info' is uninitialized, and the uninitialized value is copied to user object when calling PANTHOR_UOBJ_SET().	https://git.kernel.org/stable/c/3b32b7f638fe61e9d2929096017 2f4e360e38233, https://git.kernel.org/stable/c/64b95bbc08bacf3e4b05c8604e6a4fec43bb712a	O-LIN-LINU-180325/2511

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Using memset to initialize 'priorities_info' to avoid this garbage value problem. **CVE ID: CVE-2025-21843**		
Affected Version(s): From (including) 6.13 Up to (excluding) 6.13.5					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/ism: add release function for struct device According to device_release() in /drivers/base/core.c, a device without a release function is a broken device and must be fixed. The current code directly frees the device after calling device_add() without waiting for other kernel parts to release their references. Thus, a reference could still be held to a struct device, e.g., by sysfs, leading to potential use-after-free issues if a proper release function is not set. **CVE ID: CVE-2025-21856**	https://git.kernel.org/stable/c/0505ff2936f166405d81d0d454a81d9c14124344, https://git.kernel.org/stable/c/915e34d5ad35a6a9e56113f852ade4a730fb88f0, https://git.kernel.org/stable/c/940d15254d2216b585558bcf36312da50074e711	O-LIN-LINU-180325/2512
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Don't reference skb after sending to VIOS Previously, after successfully flushing the xmit buffer to VIOS, the tx_bytes stat was incremented by the length of the skb. It is invalid to access the skb memory after sending the buffer to	https://git.kernel.org/stable/c/093b0e5c90592773863f300b908b741622eef597, https://git.kernel.org/stable/c/25dddd01dcc8ef3acff964dbb32eeb0d89f098e9, https://git.kernel.org/stable/c/501ac6a7e21b82e05207c6b4449812d82820f306	O-LIN-LINU-180325/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the VIOS because, at any point after sending, the VIOS can trigger an interrupt to free this memory. A race between reading skb->len and freeing the skb is possible (especially during LPM) and will result in use-after-free: ========== ========== ========== === BUG: KASAN: slab-use-after-free in ibmvnic_xmit+0x75c/0x1808 [ibmvnic] Read of size 4 at addr c00000024eb48a70 by task hxecom/14495 <...> Call Trace: [c000000118f66cf0] [c0000000018cba6c] dump_stack_lvl+0x84/0xe8 (unreliable) [c000000118f66d20] [c0000000006f0080] print_report+0x1a8/0x7f0 [c000000118f66df0] [c0000000006f08f0] kasan_report+0x128/0x1f8 [c000000118f66f00] [c0000000006f2868] __asan_load4+0xac/0xe0 [c000000118f66f20] [c0080000046eac84] ibmvnic_xmit+0x75c/0x1808 [ibmvnic] [c000000118f67340] [c0000000014be168] dev_hard_start_xmit+0x150/0x358 <...> Freed by task 0: kasan_save_stack+0x34/0x68 kasan_save_track+0x2c/0x5		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 kasan_save_free_info+0x64/0x108 __kasan_mempool_poison_object+0x148/0x2d4 napi_skb_cache_put+0x5c/0x194 net_tx_action+0x154/0x5b8 handle_softirqs+0x20c/0x60c do_softirq_own_stack+0x6c/0x88 <...> The buggy address belongs to the object at c00000024eb48a00 which belongs to the cache skbuff_head_cache of size 224 ========== ========== ========== === **CVE ID: CVE-2025-21855**		
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller reported a use-after-free in geneve_find_dev() [0] without repro. geneve_configure() links struct geneve_dev.next to net_generic(net, geneve_net_id)->geneve_list. The net here could differ from dev_net(dev) if	https://git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf, https://git.kernel.org/stable/c/5a0538ac6826807d6919f6aecbb8996c2865af2c, https://git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	O-LIN-LINU-180325/2514

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IFLA_NET_NS_PID, IFLA_NET_NS_FD, or IFLA_TARGET_NETNSID is set. When dev_net(dev) is dismantled, geneve_exit_batch_rtnl() finally calls unregister_netdevice_queue() for each dev in the netns, and later the dev is freed. However, its geneve_dev.next is still linked to the backend UDP socket netns. Then, use-after-free will occur when another geneve dev is created in the netns. Let's call geneve_dellink() instead in geneve_destroy_tunnels(). [0]: BUG: KASAN: slab-use-after-free in geneve_find_dev drivers/net/geneve.c:1295 [inline] BUG: KASAN: slab-use-after-free in geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 Read of size 2 at addr ffff000054d6ee24 by task syz.1.4029/13441 CPU: 1 UID: 0 PID: 13441 Comm: syz.1.4029 Not tainted 6.13.0-g0ad9617c78ac #24 dc35ca22c79fb82e8e7bc5c9c9adafea898b1e3d Hardware name: linux,dummy-virt (DT) Call trace: show_stack+0x38/0x50		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/arm64/kernel/stacktrace.c:466 (C) __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xbc/0x108 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x16c/0x6f0 mm/kasan/report.c:489 kasan_report+0xc0/0x120 mm/kasan/report.c:602 __asan_report_load2_noabort+0x20/0x30 mm/kasan/report_generic.c:379 geneve_find_dev drivers/net/geneve.c:1295 [inline] geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 geneve_newlink+0xb8/0x128 drivers/net/geneve.c:1634 rtnl_newlink_create+0x23c/0x868 net/core/rtnetlink.c:3795 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x618/0x838 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x5fc/0x8b0 net/netlink/af_netlink.c:1892 sock_sendmsg_nosec net/socket.c:713 [inline] __sock_sendmsg net/socket.c:728 [inline] ____sys_sendmsg+0x410/0x6f8 net/socket.c:2568 ___sys_sendmsg+0x178/0x1d8 net/socket.c:2622 __sys_sendmsg net/socket.c:2654 [inline] __do_sys_sendmsg net/socket.c:2659 [inline] __se_sys_sendmsg net/socket.c:2657 [inline] __arm64_sys_sendmsg+0x12c/0x1c8 net/socket.c:2657 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x90/0x278 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x13c/0x250 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x54/0x70 arch/arm64/kernel/syscall.c:151 el0_svc+0x4c/0xa8 arch/arm64/kernel/entry-common.c:744 el0t_64_sync_handler+0x78		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/0x108 arch/arm64/kernel/entry-common.c:762 el0t_64_sync+0x198/0x1a0 arch/arm64/kernel/entry.S:600 Allocated by task 13247: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x68 mm/kasan/common.c:68 kasan_save_alloc_info+0x44/0x58 mm/kasan/generic.c:568 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x84/0xa0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4298 [inline] __kmalloc_node_noprof+0x2a0/0x560 mm/slub.c:4304 __kvmalloc_node_noprof+0x9c/0x230 mm/util.c:645 alloc_netdev_mqs+0xb8/0x11a0 net/core/dev.c:11470 rtnl_create_link+0x2b8/0xb50 net/core/rtnetlink.c:3604 rtnl_newlink_create+0x19c/0x868 net/core/rtnetlink.c:3780 __rtnl_newlink net/core/rtnetlink.c:3906 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_n ---truncated--- **CVE ID: CVE-2025-21858**		
N/A	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: io_uring: prevent opcode speculation sqe->opcode is used for different tables, make sure we santitise it against speculations. **CVE ID: CVE-2025-21863**	https://git.kernel.org/stable/c/1e988c3fe1264708f4f92109203ac5b1d65de50b, https://git.kernel.org/stable/c/506b9b5e8c2d2a411ea8fe361333f5081c56d23a, https://git.kernel.org/stable/c/b9826e3b26ec031e9063f64a7c735449c43955e4	O-LIN-LINU-180325/2515
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: f_midi: f_midi_complete to call queue_work When using USB MIDI, a lock is attempted to be acquired twice through a re-entrant call to f_midi_transmit, causing a deadlock.	https://git.kernel.org/stable/c/1f10923404705a94891e612dff3b75e828a78368, https://git.kernel.org/stable/c/24a942610ee9bafb2692a456ae850c5b2e409b05, https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2516

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix it by using queue_work() to schedule the inner f_midi_transmit() via a high priority work queue from the completion handler. **CVE ID: CVE-2025-21859**	4ab37fcb42832cdd3e9d5e50653285ca84d6686f	
Use After Free	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/migrate_device: don't add folio to be freed to LRU in migrate_device_finalize() If migration succeeded, we called folio_migrate_flags()->mem_cgroup_migrate() to migrate the memcg from the old to the new folio. This will set memcg_data of the old folio to 0. Similarly, if migration failed, memcg_data of the dst folio is left unset. If we call folio_putback_lru() on such folios (memcg_data == 0), we will add the folio to be freed to the LRU, making memcg code unhappy. Running the hmm selftests: # ./hmm-tests ... # RUN hmm.hmm_device_private.migrate ... [102.078007][T14893] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x7ff27d200 pfn:0x13cc00 [102.079974][T14893] anon flags:	https://git.kernel.org/stable/c/069dd21ea8262204f94737878389c2815a054a9e, https://git.kernel.org/stable/c/3f9240d59e9a95d19f06120bfd1d0e681c6c0ac7, https://git.kernel.org/stable/c/41cddf83d8b00f29fd105e7a0777366edc69a5cf	O-LIN-LINU-180325/2517

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x17ff00000020018(uptodate|dirty|swapbacked|node=0|zone=2|lastcpupid=0x7ff) [102.082037][T14893] raw: 017ff00000020018 dead000000000100 dead000000000122 ffff8881353896c9 [102.083687][T14893] raw: 00000007ff27d200 0000000000000000 00000001ffffffff 0000000000000000 [102.085331][T14893] page dumped because: VM_WARN_ON_ONCE_FOLIO(!memcg && !mem_cgroup_disabled()) [102.087230][T14893] ------------[cut here]------------ [102.088279][T14893] WARNING: CPU: 0 PID: 14893 at ./include/linux/memcontrol.h:726 folio_lruvec_lock_irqsave+0x10e/0x170 [102.090478][T14893] Modules linked in: [102.091244][T14893] CPU: 0 UID: 0 PID: 14893 Comm: hmm-tests Not tainted 6.13.0-09623-g6c216bc522fd #151 [102.093089][T14893] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 [102.094848][T14893] RIP: 0010:folio_lruvec_lock_irqsave+0x10e/0x170 [102.096104][T14893] Code: ... [102.099908][T14893] RSP: 0018:ffffc900236c37b0 EFLAGS: 00010293 [102.101152][T14893] RAX: 0000000000000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RBX: ffffea0004f30000 RCX: ffffffff8183f426 [102.102684][T14893] RDX: ffff8881063cb880 RSI: ffffffff81b8117f RDI: ffff8881063cb880 [102.104227][T14893] RBP: 0000000000000000 R08: 0000000000000005 R09: 0000000000000000 [102.105757][T14893] R10: 0000000000000001 R11: 0000000000000002 R12: ffffc900236c37d8 [102.107296][T14893] R13: ffff888277a2bcb0 R14: 000000000000001f R15: 0000000000000000 [102.108830][T14893] FS: 00007ff27dbdd740(0000) GS:ffff888277a00000(0000) knlGS:0000000000000000 [102.110643][T14893] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [102.111924][T14893] CR2: 00007ff27d400000 CR3: 000000010866e000 CR4: 0000000000750ef0 [102.113478][T14893] PKRU: 55555554 [102.114172][T14893] Call Trace: [102.114805][T14893] <TASK> [102.115397][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.116547][T14893] ? __warn.cold+0x110/0x210 [102.117461][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.118667][T14893] ? report_bug+0x1b9/0x320 [102.119571][T14893] ? handle_bug+0x54/0x90 [102.120494][T14893] ? exc_invalid_op+0x17/0x50 [102.121433][T14893] ?		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			asm_exc_invalid_op+0x1a/0x20 [102.122435][T14893] ? __wake_up_klogd.part.0+0x76/0xd0 [102.123506][T14893] ? dump_page+0x4f/0x60 [102.124352][T14893] ? folio_lruvec_lock_irqsave+0x10e/0x170 [102.125500][T14893] folio_batch_move_lru+0xd4/0x200 [102.126577][T14893] ? __pfx_lru_add+0x10/0x10 [102.127505][T14893] __folio_batch_add_and_move+0x391/0x720 [102.128633][T14893] ? __pfx_lru_add+0x10/0x10 [102.129550][T14893] folio_putback_lru+0x16/0x80 [102.130564][T14893] migrate_device_finalize+0x9b/0x530 [102.131640][T14893] dmirror_migrate_to_device.constprop.0+0x7c5/0xad0 [102.133047][T14893] dmirror_fops_unlocked_ioctl+0x89b/0xc80 Likely, nothing else goes wrong: putting the last folio reference will remove the folio from the LRU again. So besides memcg complaining, adding the folio to be freed to the LRU is just an unnecessary step. The new flow resembles what we have in migrate_folio_move(): add the dst to the lru, rem ---truncated--- **CVE ID: CVE-2025-21861**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink(). [device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2518

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue (). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00 /0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object] RSP: process kstack fffffe8040b4fbd0+0x7bd0/0x8000 [kworker/u8:7+netns 1804]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R09: kasan shadow of process kstack ffffffe8040b4f990+0x7990/ 0x8000 [kworker/u8:7+netns 1804] R10: process kstack ffffffe8040b4f997+0x7997/ 0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_ core_dev_11127_8_1328_8_ S_4096_A_64_n_139+0xc08 /0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 ffffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK> [<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] ffffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] ffffffe8040b4fc28 [<ffffffff8a0c360d>] list_del		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop dst Xiumei reported hitting the WARN in xfrm6_tunnel_net_exit while running tests that boil down to: - create a pair of netns - run a basic TCP test over ipcomp6 - delete the pair of netns The xfrm_state found on spi_byaddr was not deleted at the time we delete the netns, because we still have a reference on it. This lingering reference comes from a secpath (which holds a ref on the xfrm_state), which is still attached to an skb. This skb is not leaked, it ends up on sk_receive_queue and then gets defer-free'd by skb_attempt_defer_free. The problem happens when we defer freeing an skb (push it on one CPU's defer_list), and don't flush that list before the netns is deleted. In that case, we still have a reference on the xfrm_state that we don't expect at this point. We already drop the skb's	https://git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9, https://git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491, https://git.kernel.org/stable/c/9b6412e6979f6f9e0632075f8f008937b5cd4efd	O-LIN-LINU-180325/2519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dst in the TCP receive path when it's no longer needed, so let's also drop the secpath. At this point, tcp_filter has already called into the LSM hooks that may require the secpath, so it should not be needed anymore. However, in some of those places, the MPTCP extension has just been attached to the skb, so we cannot simply drop all extensions. **CVE ID: CVE-2025-21864**		
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/code-patching: Fix KASAN hit by not flagging text patching area as VM_ALLOC Erhard reported the following KASAN hit while booting his PowerMac G4 with a KASAN-enabled kernel 6.13-rc6: BUG: KASAN: vmalloc-out-of-bounds in copy_to_kernel_nofault+0xd8/0x1c8 Write of size 8 at addr f1000000 by task chronyd/1293 CPU: 0 UID: 123 PID: 1293 Comm: chronyd Tainted: G W 6.13.0-rc6-PMacG4 #2 Tainted: [W]=WARN Hardware name: PowerMac3,6 7455 0x80010303 PowerMac Call Trace: [c2437590] [c1631a84]	https://git.kernel.org/stable/c/2d542f13d26344e3452eee77613026ce9b653065, https://git.kernel.org/stable/c/2e6c80423f201405fd65254e52decd21663896f3, https://git.kernel.org/stable/c/6847b3e40bb963e57b61d1cc6fe84cb37b9d3d4c	O-LIN-LINU-180325/2520

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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+0x70/0x8c (unreliable) [c24375b0] [c0504998] print_report+0xdc/0x504 [c2437610] [c050475c] kasan_report+0xf8/0x108 [c2437690] [c0505a3c] kasan_check_range+0x24/0x18c [c24376a0] [c03fb5e4] copy_to_kernel_nofault+0xd8/0x1c8 [c24376c0] [c004c014] patch_instructions+0x15c/0x16c [c2437710] [c00731a8] bpf_arch_text_copy+0x60/0x7c [c2437730] [c0281168] bpf_jit_binary_pack_finalize+0x50/0xac [c2437750] [c0073cf4] bpf_int_jit_compile+0xb30/0xdec [c2437880] [c0280394] bpf_prog_select_runtime+0x15c/0x478 [c24378d0] [c1263428] bpf_prepare_filter+0xbf8/0xc14 [c2437990] [c12677ec] bpf_prog_create_from_user+0x258/0x2b4 [c24379d0] [c027111c] do_seccomp+0x3dc/0x1890 [c2437ac0] [c001d8e0] system_call_exception+0x2dc/0x420 [c2437f30] [c00281ac] ret_from_syscall+0x0/0x2c --- interrupt: c00 at 0x5a1274 NIP: 005a1274 LR: 006a3b3c CTR: 005296c8 REGS: c2437f40 TRAP: 0c00 Tainted: G W (6.13.0-rc6-PMacG4) MSR: 0200f932 <VEC,EE,PR,FP,ME,IR,DR,RI> CR: 24004422 XER: 00000000		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GPR00: 00000166 af8f3fa0 a7ee3540 00000001 00000000 013b6500 005a5858 0200f932 GPR08: 00000000 00001fe9 013d5fc8 005296c8 2822244c 00b2fcd8 00000000 af8f4b57 GPR16: 00000000 00000001 00000000 00000000 00000000 00000001 00000000 00000002 GPR24: 00afdbb0 00000000 00000000 00000000 006e0004 013ce060 006e7c1c 00000001 NIP [005a1274] 0x5a1274 LR [006a3b3c] 0x6a3b3c --- interrupt: c00 The buggy address belongs to the virtual mapping at [f1000000, f1002000) created by: text_area_cpu_up+0x20/0x190 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x76e30 flags: 0x80000000(zone=2) raw: 80000000 00000000 00000122 00000000 00000000 00000000 ffffffff 00000001 raw: 00000000 page dumped because: kasan: bad access detected Memory state around the buggy address: f0ffff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
			f0ffff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >f1000000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ f1000080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f1000100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ========== f8 corresponds to KASAN_VMALLOC_INVALID which means the area is not initialised hence not supposed to be used yet. Powerpc text patching infrastructure allocates a virtual memory area using get_vm_area() and flags it as VM_ALLOC. But that flag is meant to be used for vmalloc() and vmalloc() allocated memory is not supposed to be used before a call to __vmalloc_node_range() which is never called for that area. That went undetected until commit e4137f08816b ("mm, kasan, kmsan: instrument copy_from/to_kernel_nofault") The area allocated by text_area_cpu_up() is not vmalloc memory, it is mapped directly on demand when needed by map_kernel_page(). There is no VM flag corresponding to such usage, so just pass no		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flag. That way the area will be unpoisonned and usable immediately. **CVE ID: CVE-2025-21866**		
Use of Uninitialized Resource	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix incorrect initialization order Syzkaller reports the following bug: BUG: spinlock bad magic on CPU#1, syz-executor.0/7995 lock: 0xffff88805303f3e0, .magic: 00000000, .owner: <none>/-1, .owner_cpu: 0 CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted: G E 5.10.209+ #1 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x119/0x179 lib/dump_stack.c:118 debug_spin_lock_before kernel/locking/spinlock_debug.c:83 [inline] do_raw_spin_lock+0x1f6/0x270 kernel/locking/spinlock_debug.c:112 __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:117 [inline] _raw_spin_lock_irqsave+0x50/0x70 kernel/locking/spinlock.c:159	https://git.kernel.org/stable/c/07b598c0e6f06a0f254c88dafb4ad50f8a8c6eea, https://git.kernel.org/stable/c/0efa6c42f81c60d8f72ba7f5ed8d4fec8c526282, https://git.kernel.org/stable/c/219a47d0e6195bd202f22855e35f25bd15bc4d58	O-LIN-LINU-180325/2521

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reset_per_cpu_data+0xe6/0x240 [drop_monitor] net_dm_cmd_trace+0x43d/0x17a0 [drop_monitor] genl_family_rcv_msg_doit+0x22f/0x330 net/netlink/genetlink.c:739 genl_family_rcv_msg net/netlink/genetlink.c:783 [inline] genl_rcv_msg+0x341/0x5a0 net/netlink/genetlink.c:800 netlink_rcv_skb+0x14d/0x440 net/netlink/af_netlink.c:2497 genl_rcv+0x29/0x40 net/netlink/genetlink.c:811 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x54b/0x800 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x914/0xe00 net/netlink/af_netlink.c:1916 sock_sendmsg_nosec net/socket.c:651 [inline] __sock_sendmsg+0x157/0x190 net/socket.c:663 ___sys_sendmsg+0x712/0x870 net/socket.c:2378 __sys_sendmsg+0xf8/0x170 net/socket.c:2432 __sys_sendmsg+0xea/0x1b0 net/socket.c:2461 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			46 entry_SYSCALL_64_after_hwframe+0x62/0xc7 RIP: 0033:0x7f3f9815aee9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3f972bf0c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f3f9826d050 RCX: 00007f3f9815aee9 RDX: 0000000020000000 RSI: 0000000020001300 RDI: 0000000000000007 RBP: 00007f3f981b63bd R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f3f9826d050 R15: 00007ffe01ee6768 If drop_monitor is built as a kernel module, syzkaller may have time to send a netlink NET_DM_CMD_START message during the module loading. This will call the net_dm_monitor_start() function that uses a spinlock that has not yet been initialized. To fix this, let's place resource initialization above the registration of a generic netlink family. Found by InfoTeCS on behalf		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Linux Verification Center (linuxtesting.org) with Syzkaller. **CVE ID: CVE-2025-21862**		
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: mtd: spi-nor: sst: Fix SST write failure 'commit 18bcb4aa54ea ("mtd: spi-nor: sst: Factor out common write operation to `sst_nor_write_data()`")' introduced a bug where only one byte of data is written, regardless of the number of bytes passed to sst_nor_write_data(), causing a kernel crash during the write operation. Ensure the correct number of bytes are written as passed to sst_nor_write_data(). Call trace: [57.400180] ------------[cut here]------------ [57.404842] While writing 2 byte written 1 bytes [57.409493] WARNING: CPU: 0 PID: 737 at drivers/mtd/spi-nor/sst.c:187 sst_nor_write_data+0x6c/0x74 [57.418464] Modules linked in: [57.421517] CPU: 0 UID: 0 PID: 737 Comm: mtd_debug Not tainted 6.12.0-g5ad04afd91f9 #30 [57.429517] Hardware name: Xilinx Versal A2197 Processor board revA - x-prc-02 revA (DT) [57.437600] pstate:	https://git.kernel.org/stable/c/539bd20352832b9244238a055eb169ccf1c41ff6, https://git.kernel.org/stable/c/9553391f32f8c43e12fc7c04e1035160b5ea20bf, https://git.kernel.org/stable/c/bb1accc7e0f688886f0c634f2e878b8ac4ee6a58	O-LIN-LINU-180325/2522

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [57.444557] pc : sst_nor_write_data+0x6c/0x74 [57.448911] lr : sst_nor_write_data+0x6c/0x74 [57.453264] sp : ffff80008232bb40 [57.456570] x29: ffff80008232bb40 x28: 0000000000010000 x27: 0000000000000001 [57.463708] x26: 000000000000ffff x25: 0000000000000000 x24: 0000000000000000 [57.470843] x23: 0000000000010000 x22: ffff80008232bbf0 x21: ffff000816230000 [57.477978] x20: ffff0008056c0080 x19: 0000000000000002 x18: 0000000000000006 [57.485112] x17: 0000000000000000 x16: 0000000000000000 x15: ffff80008232b580 [57.492246] x14: 0000000000000000 x13: ffff8000816d1530 x12: 00000000000004a4 [57.499380] x11: 000000000000018c x10: ffff8000816fd530 x9 : ffff8000816d1530 [57.506515] x8 : 00000000fffff7ff x7 : ffff8000816fd530 x6 : 0000000000000001 [57.513649] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [57.520782] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0008049b0000 [57.527916] 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
			[57.530354] sst_nor_write_data+0x6c/0x74 [57.534361] sst_nor_write+0xb4/0x18c [57.538019] mtd_write_oob_std+0x7c/0x88 [57.541941] mtd_write_oob+0x70/0xbc [57.545511] mtd_write+0x68/0xa8 [57.548733] mtdchar_write+0x10c/0x290 [57.552477] vfs_write+0xb4/0x3a8 [57.555791] ksys_write+0x74/0x10c [57.559189] __arm64_sys_write+0x1c/0x28 [57.563109] invoke_syscall+0x54/0x11c [57.566856] el0_svc_common.constprop.0+0xc0/0xe0 [57.571557] do_el0_svc+0x1c/0x28 [57.574868] el0_svc+0x30/0xcc [57.577921] el0t_64_sync_handler+0x120/0x12c [57.582276] el0t_64_sync+0x190/0x194 [57.585933] ---[end trace 0000000000000000]--- [pratyush@kernel.org: add Cc stable tag] **CVE ID: CVE-2025-21845**		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix deadlock when freeing cgroup storage The following commit	https://git.kernel.org/stable/c/6ecb9fa14eec5f15d97c84c36896871335f6ddfb, https://git.kernel.org/stable/c/c78f4afbd962f4	O-LIN-LINU-180325/2523

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bc235cdb423a ("bpf: Prevent deadlock from recursive bpf_task_storage_[get|delete]") first introduced deadlock prevention for fentry/fexit programs attaching on bpf_task_storage helpers. That commit also employed the logic in map free path in its v6 version. Later bpf_cgrp_storage was first introduced in c4bcfb38a95e ("bpf: Implement cgroup storage available to non-cgroup-attached bpf progs") which faces the same issue as bpf_task_storage, instead of its busy counter, NULL was passed to bpf_local_storage_map_free() which opened a window to cause deadlock: <TASK> (acquiring local_storage->lock) _raw_spin_lock_irqsave+0x3d/0x50 bpf_local_storage_update+0xd1/0x460 bpf_cgrp_storage_get+0x109/0x130 bpf_prog_a4d4a370ba857314_cgrp_ptr+0x139/0x170 ? __bpf_prog_enter_recur+0x16/0x80 bpf_trampoline_6442485186+0x43/0xa4 cgroup_storage_ptr+0x9/0x20 (holding local_storage->lock) bpf_selem_unlink_storage_nolock.constprop.0+0x135/0x160 bpf_selem_unlink_st	3a3989f45f3ca04300252b19b5, https://git.kernel.org/stable/c/fac674d2bd68f3479f27328626b42d1eebd11fef	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			orage+0x6f/0x110 bpf_local_storage_map_free+0xa2/0x110 bpf_map_free_deferred+0x5b/0x90 process_one_work+0x17c/0x390 worker_thread+0x251/0x360 kthread+0xd2/0x100 ret_from_fork+0x34/0x50 ret_from_fork_asm+0x1a/0x30 </TASK> Progs: - A: SEC("fentry/cgroup_storage_ptr") - cgid (BPF_MAP_TYPE_HASH) Record the id of the cgroup the current task belonging to in this hash map, using the address of the cgroup as the map key. - cgrpa (BPF_MAP_TYPE_CGRP_STORAGE) If current task is a kworker, lookup the above hash map using function parameter @owner as the key to get its corresponding cgroup id which is then used to get a trusted pointer to the cgroup through bpf_cgroup_from_id(). This trusted pointer can then be passed to bpf_cgrp_storage_get() to finally trigger the deadlock issue. - B: SEC("tp_btf/sys_enter")		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			- cgrpb (BPF_MAP_TYPE_CGRP_STORAGE) The only purpose of this prog is to fill Prog A's hash map by calling bpf_cgrp_storage_get() for as many userspace tasks as possible. Steps to reproduce: - Run A; - while (true) { Run B; Destroy B; } Fix this issue by passing its busy counter to the free procedure so it can be properly incremented before storage/smap locking. **CVE ID: CVE-2024-58088**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard() Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard() to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2524
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix double accounting race when btrfs_run_delalloc_range() failed	https://git.kernel.org/stable/c/0283ee1912c8e243c931f4ee5b3672e954fe0384, https://git.kernel.org/stable/c/21333148b5c9e	O-LIN-LINU-180325/2525

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[BUG] When running btrfs with block size (4K) smaller than page size (64K, aarch64), there is a very high chance to crash the kernel at generic/750, with the following messages: (before the call traces, there are 3 extra debug messages added) BTRFS warning (device dm-3): read-write for sector size 4096 with page size 65536 is experimental BTRFS info (device dm-3): checking UUID tree hrtimer: interrupt took 5451385 ns BTRFS error (device dm-3): cow_file_range failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): run_delalloc_nocow failed, root=4957 inode=257 start=1605632 len=69632: -28 BTRFS error (device dm-3): failed to run delalloc range, root=4957 ino=257 folio=1572864 submit_bitmap=8-15 start=1605632 len=69632: -28 ------------[cut here]------------ WARNING: CPU: 2 PID: 3020984 at ordered-data.c:360 can_finish_ordered_extent+0x370/0x3b8 [btrfs] CPU: 2 UID: 0 PID: 3020984 Comm: kworker/u24:1 Tainted: G OE 6.13.0-rc1-custom+ #89 Tainted: [O]=OOT_MODULE, [E]=UNSIGNED_MODULE	52f41fafcedec3810b56a5e0e40, https://git.kernel.org/stable/c/72dad8e377afa50435940adfb697e070d3556670	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: events_unbound btrfs_async_reclaim_data_space [btrfs] pc : can_finish_ordered_extent+0x370/0x3b8 [btrfs] lr : can_finish_ordered_extent+0x1ec/0x3b8 [btrfs] Call trace: can_finish_ordered_extent+0x370/0x3b8 [btrfs] (P) can_finish_ordered_extent+0x1ec/0x3b8 [btrfs] (L) btrfs_mark_ordered_io_finished+0x130/0x2b8 [btrfs] extent_writepage+0x10c/0x3b8 [btrfs] extent_write_cache_pages+0x21c/0x4e8 [btrfs] btrfs_writepages+0x94/0x160 [btrfs] do_writepages+0x74/0x190 filemap_fdatawrite_wbc+0x74/0xa0 start_delalloc_inodes+0x17c/0x3b0 [btrfs] btrfs_start_delalloc_roots+0x17c/0x288 [btrfs] shrink_delalloc+0x11c/0x280 [btrfs] flush_space+0x288/0x328 [btrfs] btrfs_async_reclaim_data_space+0x180/0x228 [btrfs]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process_one_work+0x228/0x680 worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1605632 OE len=16384 to_dec=16384 left=0 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1622016 OE len=12288 to_dec=12288 left=0 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 BTRFS critical (device dm-3): bad ordered extent accounting, root=4957 ino=257 OE offset=1634304 OE len=8192 to_dec=4096 left=0 CPU: 1 UID: 0 PID: 3286940 Comm: kworker/u24:3 Tainted: G W OE 6.13.0-rc1-custom+ #89 Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 Workqueue: btrfs_work_helper [btrfs] (btrfs-endio-write) pstate: 404000c5 (nZcv daIF +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : process_one_work+0x110/0x680 lr : worker_thread+0x1bc/0x360 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
			process_one_work+0x110/0x680 (P) worker_thread+0x1bc/0x360 (L) worker_thread+0x1bc/0x360 kthread+0x100/0x118 ret_from_fork+0x10/0x20 Code: f84086a1 f9000fe1 53041c21 b9003361 (f9400661) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception SMP: stopping secondary CPUs SMP: failed to stop secondary CPUs 2-3 Dumping ftrace buffer: (ftrace buffer empty) Kernel Offset: 0x275bb9540000 from 0xffff800080000000 PHYS_OFFSET: 0xffff8fbba0000000 CPU features: 0x100,00000070,00801250,8201720b [CAUSE] The above warning is triggered immediately after the delalloc range failure, this happens in the following sequence: - Range [1568K, 1636K) is dirty 1536K 1568K 1600K 1636K 1664K | |/////////\////////| | Where 1536K, 1600K and 1664K are page boundaries (64K page size) - Enter extent_writepage()		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for page 1536K - Enter run_delalloc_nocow() with locke ---truncated--- **CVE ID: CVE-2024-58089**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: acct: perform last write from workqueue In [1] it was reported that the acct(2) system call can be used to trigger NULL deref in cases where it is set to write to a file that triggers an internal lookup. This can e.g., happen when pointing acc(2) to /sys/power/resume. At the point the where the write to this file happens the calling task has already exited and called exit_fs(). A lookup will thus trigger a NULL-deref when accessing current->fs. Reorganize the code so that the the final write happens from the workqueue but with the caller's credentials. This preserves the (strange) permission model and has almost no regression risk. This api should stop to exist though. **CVE ID: CVE-2025-21846**	https://git.kernel.org/stable/c/56d5f3eba3f5de0efdd556de4ef381e109b973a9, https://git.kernel.org/stable/c/5a59ced8ffc71973d42c82484a719c8f6ac8f7f7, https://git.kernel.org/stable/c/5c928e14a2ccd99462f2351ead627b58075bb736	O-LIN-LINU-180325/2526
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/2b3878baf9091	O-LIN-LINU-180325/2527

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ASoC: SOF: stream-ipc: Check for cstream nullity in sof_ipc_msg_data() The nullity of sps->cstream should be checked similarly as it is done in sof_set_stream_data_offset() function. Assuming that it is not NULL if sps->stream is NULL is incorrect and can lead to NULL pointer dereference. **CVE ID: CVE-2025-21847**	8a361a3dfd3513025100b1b40b6, https://git.kernel.org/stable/c/62ab1ae5511c59b5f0bf550136ff321331adca9f, https://git.kernel.org/stable/c/6c18f5eb2043ebf4674c08a9690218dc818a11ab	
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: sockmap, vsock: For connectible sockets allow only connected sockmap expects all vsocks to have a transport assigned, which is expressed in vsock_proto::psock_update_sk_prot(). However, there is an edge case where an unconnected (connectible) socket may lose its previously assigned transport. This is handled with a NULL check in the vsock/BPF recv path. Another design detail is that listening vsocks are not supposed to have any transport assigned at all. Which implies they are not supported by the sockmap. But this is complicated by the fact that a socket, before switching to TCP_LISTEN, may have had some transport assigned during a	https://git.kernel.org/stable/c/22b683217ad2112791a708693cb236507abd637a, https://git.kernel.org/stable/c/8fb5bb169d17cdd12c2dcc2e96830ed487d77a0f, https://git.kernel.org/stable/c/cc9a7832ede53ade1ba9991f0e27314caa4029d8	O-LIN-LINU-180325/2528

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			failed connect() attempt. Hence, we may end up with a listening vsock in a sockmap, which blows up quickly: KASAN: null-ptr-deref in range [0x0000000000000120-0x0000000000000127] CPU: 7 UID: 0 PID: 56 Comm: kworker/7:0 Not tainted 6.14.0-rc1+ Workqueue: vsock-loopback vsock_loopback_work RIP: 0010:vsock_read_skb+0x4b/0x90 Call Trace: sk_psock_verdict_data_ready+0xa4/0x2e0 virtio_transport_recv_pkt+0x1ca8/0x2acc vsock_loopback_work+0x27d/0x3f0 process_one_work+0x846/0x1420 worker_thread+0x5b3/0xf80 kthread+0x35a/0x700 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x1a/0x30 For connectible sockets, instead of relying solely on the state of vsk->transport, tell sockmap to only allow those representing established connections. This aligns with the behaviour for AF_INET and AF_UNIX. **CVE ID: CVE-2025-21854**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: avoid holding freeze_mutex during mmap operation We use map->freeze_mutex to prevent races between map_freeze() and memory mapping BPF map contents with writable permissions. The way we naively do this means we'll hold freeze_mutex for entire duration of all the mm and VMA manipulations, which is completely unnecessary. This can potentially also lead to deadlocks, as reported by syzbot in [0]. So, instead, hold freeze_mutex only during writeability checks, bump (proactively) "write active" count for the map, unlock the mutex and proceed with mmap logic. And only if something went wrong during mmap logic, then undo that "write active" counter increment. [0] https://lore.kernel.org/bpf/678dcbc9.050a0220.303755.0066.GAE@google.com/ **CVE ID: CVE-2025-21853**	https://git.kernel.org/stable/c/271e49f8a58edba65bc2b1250a0abaa98c4bfdbe, https://git.kernel.org/stable/c/29cfda62ab4d92ab94123813db49ab76c1e61b29, https://git.kernel.org/stable/c/bc27c52eea189e8f7492d40739b7746d67b65beb	O-LIN-LINU-180325/2529
Loop with Unreachable Exit Condition ('Infinite Loop')	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nvmet: Fix crash when a namespace is disabled The namespace percpu	https://git.kernel.org/stable/c/4082326807072b71496501b6a0c55ffe8d5092a5, https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			counter protects pending I/O, and we can only safely diable the namespace once the counter drop to zero. Otherwise we end up with a crash when running blktests/nvme/058 (eg for loop transport): [2352.930426] [T53909] Oops: general protection fault, probably for non-canonical address 0xdffffc0000000005: 0000 [#1] PREEMPT SMP KASAN PTI [2352.930431] [T53909] KASAN: null-ptr-deref in range [0x0000000000000028-0x000000000000002f] [2352.930434] [T53909] CPU: 3 UID: 0 PID: 53909 Comm: kworker/u16:5 Tainted: G W 6.13.0-rc6 #232 [2352.930438] [T53909] Tainted: [W]=WARN [2352.930440] [T53909] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-3.fc41 04/01/2014 [2352.930443] [T53909] Workqueue: nvmet-wq nvme_loop_execute_work [nvme_loop] [2352.930449] [T53909] RIP: 0010:blkcg_set_ioprio+0x44/0x180 as the queue is already torn down when calling submit_bio(); So we need to init the percpu counter in nvmet_ns_enable(), and wait for it to drop to zero in nvmet_ns_disable() to avoid	cc0607594f6813342b27c752c6fb6f6eb9980cb5	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			having I/O pending after the namespace has been disabled. **CVE ID: CVE-2025-21850**		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Use spin_lock_irqsave() in interruptible context spin_lock/unlock() functions used in interrupt contexts could result in a deadlock, as seen in GitLab issue #13399, which occurs when interrupt comes in while holding a lock. Try to remedy the problem by saving irq state before spin lock acquisition. v2: add irqs' state save/restore calls to all locks/unlocks in signal_irq_work() execution (Maciej) v3: use with spin_lock_irqsave() in guc_lrc_desc_unpin() instead of other lock/unlock calls and add Fixes and Cc tags (Tvrtko); change title and commit message (cherry picked from commit c088387ddd6482b40f21ccf23db1125e8fa4af7e) **CVE ID: CVE-2025-21849**	https://git.kernel.org/stable/c/2bf1f4c129db7a10920655b000f0292f1ee509c2, https://git.kernel.org/stable/c/47ae46ac5407646420e06b78e0dad331e56a4bb4, https://git.kernel.org/stable/c/e49477f7f78598295551d486ecc7f020d796432e	O-LIN-LINU-180325/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: fix error handling causing NULL dereference tcf_exts_miss_cookie_base_alloc() calls xa_alloc_cyclic() which can return 1 if the allocation succeeded after wrapping. This was treated as an error, with value 1 returned to caller tcf_exts_init_ex() which sets exts->actions to NULL and returns 1 to caller fl_change(). fl_change() treats err == 1 as success, calling tcf_exts_validate_ex() which calls tcf_action_init() with exts->actions as argument, where it is dereferenced. Example trace: BUG: kernel NULL pointer dereference, address: 0000000000000000 CPU: 114 PID: 16151 Comm: handler114 Kdump: loaded Not tainted 5.14.0-503.16.1.el9_5.x86_64 #1 RIP: 0010:tcf_action_init+0x1f8/0x2c0 Call Trace: tcf_action_init+0x1f8/0x2c0 tcf_exts_validate_ex+0x175/0x190 fl_change+0x537/0x1120 [cls_flower] **CVE ID: CVE-2025-21857**	https://git.kernel.org/stable/c/071ed42cff4fcdd89025d966d48eabef59913bf2, https://git.kernel.org/stable/c/3c74b5787caf59bb1e9c5fe0a360643a71eb1e8a, https://git.kernel.org/stable/c/3e4c56cf41876ef2a82f0877fe2a67648f8632b8	O-LIN-LINU-180325/2532

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: bpf: Add check for nfp_app_ctrl_msg_alloc() Add check for the return value of nfp_app_ctrl_msg_alloc() in nfp_bpf_cmsg_alloc() to prevent null pointer dereference. **CVE ID: CVE-2025-21848**	https://git.kernel.org/stable/c/1358d8e07afdf21d49ca6f00c56048442977e00a, https://git.kernel.org/stable/c/29ccb1e4040da6ff02b7e64efaa2f8e6bf06020d, https://git.kernel.org/stable/c/878e7b11736e062514e58f3b445ff343e6705537	O-LIN-LINU-180325/2533
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net: Add rx_skb of kfree_skb to raw_tp_null_args[]. Yan Zhai reported a BPF prog could trigger a null-ptr-deref [0] in trace_kfree_skb if the prog does not check if rx_sk is NULL. Commit c53795d48ee8 ("net: add rx_sk to trace_kfree_skb") added rx_sk to trace_kfree_skb, but rx_sk is optional and could be NULL. Let's add kfree_skb to raw_tp_null_args[] to let the BPF verifier validate such a prog and prevent the issue. Now we fail to load such a prog: libbpf: prog 'drop': -- BEGIN PROG LOAD LOG -- 0: R1=ctx() R10=fp0 ; int BPF_PROG(drop, struct sk_buff *skb, void *location, @	https://git.kernel.org/stable/c/4dba79c1e7aad6620bbb707b6c4459380fd90860, https://git.kernel.org/stable/c/5da7e15fb5a12e78de974d8908f348e279922ce9, https://git.kernel.org/stable/c/f579afacd0a66971fc8481f30d2d377e230a8342	O-LIN-LINU-180325/2534

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kfree_skb_sk_null.bpf.c:21 0: (79) r3 = *(u64 *)(r1 +24) func 'kfree_skb' arg3 has btf_id 5253 type STRUCT 'sock' 1: R1=ctx() R3_w=trusted_ptr_or_null_sock(id=1) ; bpf_printk("sk: %d, %d\n", sk, sk->__sk_common.skc_family); @ kfree_skb_sk_null.bpf.c:24 1: (69) r4 = *(u16 *)(r3 +16) R3 invalid mem access 'trusted_ptr_or_null_' processed 2 insns (limit 1000000) max_states_per_insn 0 total_states 0 peak_states 0 mark_read 0 -- END PROG LOAD LOG -- Note this fix requires commit 838a10bd2ebf ("bpf: Augment raw_tp arguments with PTR_MAYBE_NULL"). [0]: BUG: kernel NULL pointer dereference, address: 0000000000000010 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 0 P4D 0 PREEMPT SMP RIP: 0010:bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d Call Trace: <TASK> ? __die+0x1f/0x60 ? page_fault_oops+0x148/0x420 ? search_bpf_extables+0x5b/		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x70 ? fixup_exception+0x27/0x2c0 ? exc_page_fault+0x75/0x170 ? asm_exc_page_fault+0x22/0x30 ? bpf_prog_5e21a6db8fcff1aa_drop+0x10/0x2d bpf_trace_run4+0x68/0xd0 ? unix_stream_connect+0x1f4/0x6f0 sk_skb_reason_drop+0x90/0x120 unix_stream_connect+0x1f4/0x6f0 __sys_connect+0x7f/0xb0 __x64_sys_connect+0x14/0x20 do_syscall_64+0x47/0xc30 entry_SYSCALL_64_after_hwframe+0x4b/0x53 **CVE ID: CVE-2025-21852**		
Improper Locking	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix softlockup in arena_map_free on 64k page kernel On an aarch64 kernel with CONFIG_PAGE_SIZE_64KB=y, arena_htab tests cause a segmentation fault and soft lockup. The same failure is not observed with 4k pages on aarch64. It turns out	https://git.kernel.org/stable/c/517e8a7835e8cfb398a0aeb0133de50e31cae32b, https://git.kernel.org/stable/c/787d556a3de447e70964a4bdeba9196f62a62b1e, https://git.kernel.org/stable/c/c1f3f3892d4526f18aaeffdb6068ce861e793ee3	O-LIN-LINU-180325/2535

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arena_map_free() is calling apply_to_existing_page_range() with the address returned by bpf_arena_get_kern_vm_start(). If this address is not page-aligned the code ends up calling apply_to_pte_range() with that unaligned address causing soft lockup. Fix it by round up GUARD_SZ to PAGE_SIZE << 1 so that the division by 2 in bpf_arena_get_kern_vm_start() returns a page-aligned value. **CVE ID: CVE-2025-21851**		
N/A	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved: mm/zswap: fix inconsistency when zswap_store_page() fails Commit b7c0ccdfbafd ("mm: zswap: support large folios in zswap_store()") skips charging any zswap entries when it failed to zswap the entire folio. However, when some base pages are zswapped but it failed to zswap the entire folio, the zswap operation is rolled back. When freeing zswap entries for those pages, zswap_entry_free() uncharges the zswap entries that were not previously charged, causing zswap charging to become inconsistent. This inconsistency triggers	https://git.kernel.org/stable/c/63895d20d63b446f5049a963983489319c2ea3e2, https://git.kernel.org/stable/c/a3652f5552b20903315612da487a7be2b95394d5	O-LIN-LINU-180325/2536

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			two warnings with following steps:
			# On a machine with 64GiB of RAM and 36GiB of zswap
			$ stress-ng --bigheap 2 # wait until the OOM-killer kills stress-ng
			$ sudo reboot
			
			The two warnings are:
			in mm/memcontrol.c:163, function obj_cgroup_release():
			
			WARN_ON_ONCE(nr_bytes & (PAGE_SIZE - 1));
			
			in mm/page_counter.c:60, function page_counter_cancel():
			if (WARN_ONCE(new < 0, "page_counter underflow: %ld nr_pages=%lu\n", new, nr_pages))
			
			zswap_stored_pages also becomes inconsistent in the same way.
			
			As suggested by Kanchana, increment zswap_stored_pages and charge zswap entries within zswap_store_page() when it succeeds. This way, zswap_entry_free() will decrement the counter and uncharge the entries when it failed to zswap the entire folio.
			
			While this could potentially be optimized by batching objcg charging and incrementing the counter, let's focus on fixing the bug this time and leave the optimization for later after some evaluation.
			
			After resolving the		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inconsistency, the warnings disappear. [42.hyeyoo@gmail.com: refactor zswap_store_page()] Link: https://lkml.kernel.org/r/20250131082037.2426-1-42.hyeyoo@gmail.com **CVE ID: CVE-2025-21860**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.67					
Improper Locking	12-Mar-2025	8.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid racy issue with session expire. **CVE ID: CVE-2024-58087**	https://git.kernel.org/stable/c/2107ab40629aeabbec369cf34b8cf0f288c3eb1b, https://git.kernel.org/stable/c/37a0e2b362b3150317fb6e2139de67b1e29ae5ff, https://git.kernel.org/stable/c/450a844c045ff0895d41b05a1cbe8febd1acfcfd	O-LIN-LINU-180325/2537
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.80					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Don't reference skb after sending to VIOS Previously, after successfully flushing the xmit buffer to VIOS, the tx_bytes stat was incremented by the length of the skb. It is invalid to access the skb memory after sending the buffer to the VIOS because, at any point after sending, the VIOS can trigger an interrupt to free this	https://git.kernel.org/stable/c/093b0e5c90592773863f300b908b741622eef597, https://git.kernel.org/stable/c/25dddd01dcc8ef3acff964dbb32eeb0d89f098e9, https://git.kernel.org/stable/c/501ac6a7e21b82e05207c6b4449812d82820f306	O-LIN-LINU-180325/2538

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory. A race between reading skb->len and freeing the skb is possible (especially during LPM) and will result in use-after-free: ========== ========== ========== === BUG: KASAN: slab-use-after-free in ibmvnic_xmit+0x75c/0x1808 [ibmvnic] Read of size 4 at addr c00000024eb48a70 by task hxecom/14495 <...> Call Trace: [c000000118f66cf0] [c0000000018cba6c] dump_stack_lvl+0x84/0xe8 (unreliable) [c000000118f66d20] [c0000000006f0080] print_report+0x1a8/0x7f0 [c000000118f66df0] [c0000000006f08f0] kasan_report+0x128/0x1f8 [c000000118f66f00] [c0000000006f2868] __asan_load4+0xac/0xe0 [c000000118f66f20] [c0080000046eac84] ibmvnic_xmit+0x75c/0x1808 [ibmvnic] [c000000118f67340] [c0000000014be168] dev_hard_start_xmit+0x150/0x358 <...> Freed by task 0: kasan_save_stack+0x34/0x68 kasan_save_track+0x2c/0x50 kasan_save_free_info+0x64/0x108		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_mempool_poison_object+0x148/0x2d4 napi_skb_cache_put+0x5c/0x194 net_tx_action+0x154/0x5b8 handle_softirqs+0x20c/0x60c do_softirq_own_stack+0x6c/0x88 <...> The buggy address belongs to the object at c00000024eb48a00 which belongs to the cache skbuff_head_cache of size 224 ========== ========== ========== === **CVE ID: CVE-2025-21855**		
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller reported a use-after-free in geneve_find_dev() [0] without repro. geneve_configure() links struct geneve_dev.next to net_generic(net, geneve_net_id)->geneve_list. The net here could differ from dev_net(dev) if IFLA_NET_NS_PID, IFLA_NET_NS_FD, or IFLA_TARGET_NETNSID is set.	https://git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf, https://git.kernel.org/stable/c/5a0538ac6826807d6919f6aecbb8996c2865af2c, https://git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	O-LIN-LINU-180325/2539

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When dev_net(dev) is dismantled, geneve_exit_batch_rtnl() finally calls unregister_netdevice_queue() for each dev in the netns, and later the dev is freed. However, its geneve_dev.next is still linked to the backend UDP socket netns. Then, use-after-free will occur when another geneve dev is created in the netns. Let's call geneve_dellink() instead in geneve_destroy_tunnels(). [0]: BUG: KASAN: slab-use-after-free in geneve_find_dev drivers/net/geneve.c:1295 [inline] BUG: KASAN: slab-use-after-free in geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 Read of size 2 at addr ffff000054d6ee24 by task syz.1.4029/13441 CPU: 1 UID: 0 PID: 13441 Comm: syz.1.4029 Not tainted 6.13.0-g0ad9617c78ac #24 dc35ca22c79fb82e8e7bc5c9c9adafea898b1e3d Hardware name: linux,dummy-virt (DT) Call trace: show_stack+0x38/0x50 arch/arm64/kernel/stacktrace.c:466 (C) __dump_stack lib/dump_stack.c:94 [inline]		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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+0xbc/0x108 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x16c/0x6f0 mm/kasan/report.c:489 kasan_report+0xc0/0x120 mm/kasan/report.c:602 __asan_report_load2_noabort+0x20/0x30 mm/kasan/report_generic.c:379 geneve_find_dev drivers/net/geneve.c:1295 [inline] geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 geneve_newlink+0xb8/0x128 drivers/net/geneve.c:1634 rtnl_newlink_create+0x23c/0x868 net/core/rtnetlink.c:3795 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netlink_unicast+0x618/0x838 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x5fc/0x8b0 net/netlink/af_netlink.c:1892 sock_sendmsg_nosec net/socket.c:713 [inline] __sock_sendmsg net/socket.c:728 [inline] ___sys_sendmsg+0x410/0x6f8 net/socket.c:2568 __sys_sendmsg+0x178/0x1d8 net/socket.c:2622 __sys_sendmsg net/socket.c:2654 [inline] __do_sys_sendmsg net/socket.c:2659 [inline] __se_sys_sendmsg net/socket.c:2657 [inline] __arm64_sys_sendmsg+0x12c/0x1c8 net/socket.c:2657 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x90/0x278 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x13c/0x250 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x54/0x70 arch/arm64/kernel/syscall.c:151 el0_svc+0x4c/0xa8 arch/arm64/kernel/entry-common.c:744 el0t_64_sync_handler+0x78/0x108 arch/arm64/kernel/entry-common.c:762 el0t_64_sync+0x198/0x1a0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/arm64/kernel/entry.S :600 Allocated by task 13247: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x 68 mm/kasan/common.c:68 kasan_save_alloc_info+0x44 /0x58 mm/kasan/generic.c:568 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0x84/0xa 0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4298 [inline] __kmalloc_node_noprof+0x2 a0/0x560 mm/slub.c:4304 __kvmalloc_node_noprof+0x 9c/0x230 mm/util.c:645 alloc_netdev_mqs+0xb8/0x 11a0 net/core/dev.c:11470 rtnl_create_link+0x2b8/0xb 50 net/core/rtnetlink.c:3604 rtnl_newlink_create+0x19c/ 0x868 net/core/rtnetlink.c:3780 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x16 30 net/core/rtnetlink.c:4021		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_n ---truncated--- **CVE ID: CVE-2025-21858**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: acct: perform last write from workqueue In [1] it was reported that the acct(2) system call can be used to trigger NULL deref in cases where it is set to write to a file that triggers an internal lookup. This can e.g., happen when pointing acc(2) to /sys/power/resume. At the point the where the write to this file happens the calling task has already exited and called exit_fs(). A lookup will thus trigger a NULL-deref when accessing current->fs. Reorganize the code so that the the final write happens from the workqueue but with the caller's credentials. This preserves the (strange) permission model and has almost no regression risk.	https://git.kernel.org/stable/c/56d5f3eba3f5de0efdd556de4ef381e109b973a9, https://git.kernel.org/stable/c/5a59ced8ffc71973d42c82484a719c8f6ac8f7f7, https://git.kernel.org/stable/c/5c928e14a2ccd99462f2351ead627b58075bb736	O-LIN-LINU-180325/2540

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 api should stop to exist though. **CVE ID: CVE-2025-21846**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: bpf: Add check for nfp_app_ctrl_msg_alloc() Add check for the return value of nfp_app_ctrl_msg_alloc() in nfp_bpf_cmsg_alloc() to prevent null pointer dereference. **CVE ID: CVE-2025-21848**	https://git.kernel.org/stable/c/1358d8e07afdf21d49ca6f00c56048442977e00a, https://git.kernel.org/stable/c/29ccb1e4040da6ff02b7e64efaa2f8e6bf06020d, https://git.kernel.org/stable/c/878e7b11736e062514e58f3b445ff343e6705537	O-LIN-LINU-180325/2541
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: f_midi: f_midi_complete to call queue_work When using USB MIDI, a lock is attempted to be acquired twice through a re-entrant call to f_midi_transmit, causing a deadlock. Fix it by using queue_work() to schedule the inner f_midi_transmit() via a high priority work queue from the completion handler. **CVE ID: CVE-2025-21859**	https://git.kernel.org/stable/c/1f10923404705a94891e612dff3b75e828a78368, https://git.kernel.org/stable/c/24a942610ee9bafb2692a456ae850c5b2e409b05, https://git.kernel.org/stable/c/4ab37fcb42832cdd3e9d5e50653285ca84d6686f	O-LIN-LINU-180325/2542
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix deadlock when freeing cgroup storage The following commit	https://git.kernel.org/stable/c/6ecb9fa14eec5f15d97c84c36896871335f6ddfb, https://git.kernel.org/stable/c/c78f4afbd962f4	O-LIN-LINU-180325/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bc235cdb423a ("bpf: Prevent deadlock from recursive bpf_task_storage_[get|delete]") first introduced deadlock prevention for fentry/fexit programs attaching on bpf_task_storage helpers. That commit also employed the logic in map free path in its v6 version. Later bpf_cgrp_storage was first introduced in c4bcfb38a95e ("bpf: Implement cgroup storage available to non-cgroup-attached bpf progs") which faces the same issue as bpf_task_storage, instead of its busy counter, NULL was passed to bpf_local_storage_map_free() which opened a window to cause deadlock: <TASK> (acquiring local_storage->lock) _raw_spin_lock_irqsave+0x3d/0x50 bpf_local_storage_update+0xd1/0x460 bpf_cgrp_storage_get+0x109/0x130 bpf_prog_a4d4a370ba857314_cgrp_ptr+0x139/0x170 ? __bpf_prog_enter_recur+0x16/0x80 bpf_trampoline_6442485186+0x43/0xa4 cgroup_storage_ptr+0x9/0x20 (holding local_storage->lock) bpf_selem_unlink_storage_nolock.constprop.0+0x135/0x160 bpf_selem_unlink_st	3a3989f45f3ca04300252b19b5, https://git.kernel.org/stable/c/fac674d2bd68f3479f27328626b42d1eebd11fef	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			orage+0x6f/0x110 bpf_local_storage_map_free+0xa2/0x110 bpf_map_free_deferred+0x5b/0x90 process_one_work+0x17c/0x390 worker_thread+0x251/0x360 kthread+0xd2/0x100 ret_from_fork+0x34/0x50 ret_from_fork_asm+0x1a/0x30 </TASK> Progs: - A: SEC("fentry/cgroup_storage_ptr") - cgid (BPF_MAP_TYPE_HASH) Record the id of the cgroup the current task belonging to in this hash map, using the address of the cgroup as the map key. - cgrpa (BPF_MAP_TYPE_CGRP_STORAGE) If current task is a kworker, lookup the above hash map using function parameter @owner as the key to get its corresponding cgroup id which is then used to get a trusted pointer to the cgroup through bpf_cgroup_from_id(). This trusted pointer can then be passed to bpf_cgrp_storage_get() to finally trigger the deadlock issue. - B: SEC("tp_btf/sys_enter")		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			- cgrpb (BPF_MAP_TYPE_CGRP_STORAGE) The only purpose of this prog is to fill Prog A's hash map by calling bpf_cgrp_storage_get() for as many userspace tasks as possible. Steps to reproduce: - Run A; - while (true) { Run B; Destroy B; } Fix this issue by passing its busy counter to the free procedure so it can be properly incremented before storage/smap locking. **CVE ID: CVE-2024-58088**		
Use of Uninitialized Resource	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix incorrect initialization order Syzkaller reports the following bug: BUG: spinlock bad magic on CPU#1, syz-executor.0/7995 lock: 0xffff88805303f3e0, .magic: 00000000, .owner: <none>/-1, .owner_cpu: 0 CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted: G E 5.10.209+ #1 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: __dump_stack lib/dump_stack.c:77 [inline]	https://git.kernel.org/stable/c/07b598c0e6f06a0f254c88dafb4ad50f8a8c6eea, https://git.kernel.org/stable/c/0efa6c42f81c60d8f72ba7f5ed8d4fec8c526282, https://git.kernel.org/stable/c/219a47d0e6195bd202f22855e35f25bd15bc4d58	O-LIN-LINU-180325/2544

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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+0x119/0x179 lib/dump_stack.c:118 debug_spin_lock_before kernel/locking/spinlock_debug.c:83 [inline] do_raw_spin_lock+0x1f6/0x270 kernel/locking/spinlock_debug.c:112 __raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:117 [inline] _raw_spin_lock_irqsave+0x50/0x70 kernel/locking/spinlock.c:159 reset_per_cpu_data+0xe6/0x240 [drop_monitor] net_dm_cmd_trace+0x43d/0x17a0 [drop_monitor] genl_family_rcv_msg_doit+0x22f/0x330 net/netlink/genetlink.c:739 genl_family_rcv_msg net/netlink/genetlink.c:783 [inline] genl_rcv_msg+0x341/0x5a0 net/netlink/genetlink.c:800 netlink_rcv_skb+0x14d/0x440 net/netlink/af_netlink.c:2497 genl_rcv+0x29/0x40 net/netlink/genetlink.c:811 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x54b/0x800 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x914/0xe00		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			net/netlink/af_netlink.c:1916 sock_sendmsg_nosec net/socket.c:651 [inline] __sock_sendmsg+0x157/0x190 net/socket.c:663 ____sys_sendmsg+0x712/0x870 net/socket.c:2378 ___sys_sendmsg+0xf8/0x170 net/socket.c:2432 __sys_sendmsg+0xea/0x1b0 net/socket.c:2461 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x62/0xc7 RIP: 0033:0x7f3f9815aee9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3f972bf0c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f3f9826d050 RCX: 00007f3f9815aee9 RDX: 0000000020000000 RSI: 0000000020001300 RDI: 0000000000000007 RBP: 00007f3f981b63bd R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f3f9826d050 R15: 00007ffe01ee6768 If drop_monitor is built as a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kernel module, syzkaller may have time to send a netlink NET_DM_CMD_START message during the module loading. This will call the net_dm_monitor_start() function that uses a spinlock that has not yet been initialized. To fix this, let's place resource initialization above the registration of a generic netlink family. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with Syzkaller. **CVE ID: CVE-2025-21862**		
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/code-patching: Fix KASAN hit by not flagging text patching area as VM_ALLOC Erhard reported the following KASAN hit while booting his PowerMac G4 with a KASAN-enabled kernel 6.13-rc6: BUG: KASAN: vmalloc-out-of-bounds in copy_to_kernel_nofault+0xd8/0x1c8 Write of size 8 at addr f1000000 by task chronyd/1293 CPU: 0 UID: 123 PID: 1293 Comm: chronyd Tainted: G W 6.13.0-rc6-PMacG4 #2 Tainted: [W]=WARN	https://git.kernel.org/stable/c/2d542f13d26344e3452eee77613026ce9b653065, https://git.kernel.org/stable/c/2e6c80423f201405fd65254e52decd21663896f3, https://git.kernel.org/stable/c/6847b3e40bb963e57b61d1cc6fe84cb37b9d3d4c	O-LIN-LINU-180325/2545

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: PowerMac3,6 7455 0x80010303 PowerMac Call Trace: [c2437590] [c1631a84] dump_stack_lvl+0x70/0x8c (unreliable) [c24375b0] [c0504998] print_report+0xdc/0x504 [c2437610] [c050475c] kasan_report+0xf8/0x108 [c2437690] [c0505a3c] kasan_check_range+0x24/0x18c [c24376a0] [c03fb5e4] copy_to_kernel_nofault+0xd8/0x1c8 [c24376c0] [c004c014] patch_instructions+0x15c/0x16c [c2437710] [c00731a8] bpf_arch_text_copy+0x60/0x7c [c2437730] [c0281168] bpf_jit_binary_pack_finalize+0x50/0xac [c2437750] [c0073cf4] bpf_int_jit_compile+0xb30/0xdec [c2437880] [c0280394] bpf_prog_select_runtime+0x15c/0x478 [c24378d0] [c1263428] bpf_prepare_filter+0xbf8/0xc14 [c2437990] [c12677ec] bpf_prog_create_from_user+0x258/0x2b4 [c24379d0] [c027111c] do_seccomp+0x3dc/0x1890 [c2437ac0] [c001d8e0] system_call_exception+0x2dc/0x420 [c2437f30] [c00281ac] ret_from_syscall+0x0/0x2c --- interrupt: c00 at 0x5a1274 NIP: 005a1274 LR: 006a3b3c CTR: 005296c8 REGS: c2437f40 TRAP: 0c00 Tainted: G W (6.13.0-rc6-PMacG4)		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MSR: 0200f932 <VEC,EE,PR,FP,ME,IR,DR,RI > CR: 24004422 XER: 00000000 GPR00: 00000166 af8f3fa0 a7ee3540 00000001 00000000 013b6500 005a5858 0200f932 GPR08: 00000000 00001fe9 013d5fc8 005296c8 2822244c 00b2fcd8 00000000 af8f4b57 GPR16: 00000000 00000001 00000000 00000000 00000000 00000001 00000000 00000002 GPR24: 00afdbb0 00000000 00000000 00000000 006e0004 013ce060 006e7c1c 00000001 NIP [005a1274] 0x5a1274 LR [006a3b3c] 0x6a3b3c --- interrupt: c00 The buggy address belongs to the virtual mapping at [f1000000, f1002000) created by: text_area_cpu_up+0x20/0x190 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x76e30 flags: 0x80000000(zone=2) raw: 80000000 00000000 00000122 00000000 00000000 00000000 ffffffff 00000001 raw: 00000000 page dumped because: kasan: bad access detected		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Memory state around the buggy address: f0ffff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0ffff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >f1000000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ f1000080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f1000100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ========== ========== ========== === f8 corresponds to KASAN_VMALLOC_INVALID which means the area is not initialised hence not supposed to be used yet. Powerpc text patching infrastructure allocates a virtual memory area using get_vm_area() and flags it as VM_ALLOC. But that flag is meant to be used for vmalloc() and vmalloc() allocated memory is not supposed to be used before a call to __vmalloc_node_range() which is never called for that area. That went undetected until commit e4137f08816b ("mm, kasan, kmsan: instrument copy_from/to_kernel_nofault") The area allocated by text_area_cpu_up() is not vmalloc memory, it is		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapped directly on demand when needed by map_kernel_page(). There is no VM flag corresponding to such usage, so just pass no flag. That way the area will be unpoisonned and usable immediately. **CVE ID: CVE-2025-21866**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop dst Xiumei reported hitting the WARN in xfrm6_tunnel_net_exit while running tests that boil down to: - create a pair of netns - run a basic TCP test over ipcomp6 - delete the pair of netns The xfrm_state found on spi_byaddr was not deleted at the time we delete the netns, because we still have a reference on it. This lingering reference comes from a secpath (which holds a ref on the xfrm_state), which is still attached to an skb. This skb is not leaked, it ends up on sk_receive_queue and then gets defer-free'd by skb_attempt_defer_free. The problem happens when we defer freeing an skb (push it on one CPU's defer_list), and don't flush that list before the netns is	https://git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9, https://git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491, https://git.kernel.org/stable/c/9b6412e6979f6f9e0632075f8f008937b5cd4efd	O-LIN-LINU-180325/2546

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			deleted. In that case, we still have a reference on the xfrm_state that we don't expect at this point. We already drop the skb's dst in the TCP receive path when it's no longer needed, so let's also drop the secpath. At this point, tcp_filter has already called into the LSM hooks that may require the secpath, so it should not be needed anymore. However, in some of those places, the MPTCP extension has just been attached to the skb, so we cannot simply drop all extensions. **CVE ID: CVE-2025-21864**		
Affected Version(s): From (including) 6.3 Up to (excluding) 6.6.80					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/ism: add release function for struct device According to device_release() in /drivers/base/core.c, a device without a release function is a broken device and must be fixed. The current code directly frees the device after calling device_add() without waiting for other kernel parts to release their references. Thus, a reference could still be held to a struct device, e.g., by sysfs, leading to potential use-after-free	https://git.kernel.org/stable/c/0505ff2936f166405d81d0d454a81d9c14124344, https://git.kernel.org/stable/c/915e34d5ad35a6a9e56113f852ade4a730fb88f0, https://git.kernel.org/stable/c/940d15254d2216b585558bcf36312da50074e711	O-LIN-LINU-180325/2547

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issues if a proper release function is not set. **CVE ID: CVE-2025-21856**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: stream-ipc: Check for cstream nullity in sof_ipc_msg_data() The nullity of sps->cstream should be checked similarly as it is done in sof_set_stream_data_offset() function. Assuming that it is not NULL if sps->stream is NULL is incorrect and can lead to NULL pointer dereference. **CVE ID: CVE-2025-21847**	https://git.kernel.org/stable/c/2b3878baf90918a361a3dfd3513025100b1b40b6, https://git.kernel.org/stable/c/62ab1ae5511c59b5f0bf550136ff321331adca9f, https://git.kernel.org/stable/c/6c18f5eb2043ebf4674c08a9690218dc818a11ab	O-LIN-LINU-180325/2548
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: fix error handling causing NULL dereference tcf_exts_miss_cookie_base_alloc() calls xa_alloc_cyclic() which can return 1 if the allocation succeeded after wrapping. This was treated as an error, with value 1 returned to caller tcf_exts_init_ex() which sets exts->actions to NULL and returns 1 to caller fl_change(). fl_change() treats err == 1 as success, calling tcf_exts_validate_ex() which calls tcf_action_init() with exts->actions as argument, where it	https://git.kernel.org/stable/c/071ed42cff4fcdd89025d966d48eabef59913bf2, https://git.kernel.org/stable/c/3c74b5787caf59bb1e9c5fe0a360643a71eb1e8a, https://git.kernel.org/stable/c/3e4c56cf41876ef2a82f0877fe2a67648f8632b8	O-LIN-LINU-180325/2549

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is dereferenced. Example trace: BUG: kernel NULL pointer dereference, address: 0000000000000000 CPU: 114 PID: 16151 Comm: handler114 Kdump: loaded Not tainted 5.14.0-503.16.1.el9_5.x86_64 #1 RIP: 0010:tcf_action_init+0x1f8/0x2c0 Call Trace: tcf_action_init+0x1f8/0x2c0 tcf_exts_validate_ex+0x175/0x190 fl_change+0x537/0x1120 [cls_flower] **CVE ID: CVE-2025-21857**		
Affected Version(s): From (including) 6.4 Up to (excluding) 6.6.80					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: sockmap, vsock: For connectible sockets allow only connected sockmap expects all vsocks to have a transport assigned, which is expressed in vsock_proto::psock_update_sk_prot(). However, there is an edge case where an unconnected (connectible) socket may lose its previously assigned transport. This is handled with a NULL check in the vsock/BPF recv path. Another design detail is that listening vsocks are not supposed to have any transport assigned at all.	https://git.kernel.org/stable/c/22b683217ad2112791a708693cb236507abd637a, https://git.kernel.org/stable/c/8fb5bb169d17cdd12c2dcc2e96830ed487d77a0f, https://git.kernel.org/stable/c/cc9a7832ede53ade1ba9991f0e27314caa4029d8	O-LIN-LINU-180325/2550

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Which implies they are not supported by the sockmap. But this is complicated by the fact that a socket, before switching to TCP_LISTEN, may have had some transport assigned during a failed connect() attempt. Hence, we may end up with a listening vsock in a sockmap, which blows up quickly: KASAN: null-ptr-deref in range [0x0000000000000120-0x0000000000000127] CPU: 7 UID: 0 PID: 56 Comm: kworker/7:0 Not tainted 6.14.0-rc1+ Workqueue: vsock-loopback vsock_loopback_work RIP: 0010:vsock_read_skb+0x4b/0x90 Call Trace: sk_psock_verdict_data_ready+0xa4/0x2e0 virtio_transport_recv_pkt+0x1ca8/0x2acc vsock_loopback_work+0x27d/0x3f0 process_one_work+0x846/0x1420 worker_thread+0x5b3/0xf80 kthread+0x35a/0x700 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x1a/0x30 For connectible sockets, instead of relying solely on the state of vsk->transport, tell		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sockmap to only allow those representing established connections. This aligns with the behaviour for AF_INET and AF_UNIX. **CVE ID: CVE-2025-21854**		
Affected Version(s): From (including) 6.6.74 Up to (excluding) 6.6.80					
Out-of-bounds Write	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: gtp: Suppress list corruption splat in gtp_net_exit_batch_rtnl(). Brad Spengler reported the list_del() corruption splat in gtp_net_exit_batch_rtnl(). [0] Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for_each_netdev() loop in gtp_net_exit_batch_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit_batch_rtnl(). Say we have two netns A & B and gtp device B that resides in netns B but whose UDP socket is in netns A. 1. cleanup_net() processes netns A and then B. 2. gtp_net_exit_batch_rtnl() finds the device B while iterating netns A's gn->gtp_dev_list and calls ->dellink().	https://git.kernel.org/stable/c/33eb925c0c26e86ca540a08254806512bf911f22, https://git.kernel.org/stable/c/37e7644b961600ef0beb01d3970c3034a62913af, https://git.kernel.org/stable/c/4ccacf86491d33d2486b62d4d44864d7101b299d	O-LIN-LINU-180325/2551

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[device B is not yet unlinked from netns B as unregister_netdevice_many() has not been called.] 3. gtp_net_exit_batch_rtnl() finds the device B while iterating netns B's for_each_netdev() and calls ->dellink(). gtp_dellink() cleans up the device's hash table, unlinks the dev from gn->gtp_dev_list, and calls unregister_netdevice_queue(). Basically, calling gtp_dellink() multiple times is fine unless CONFIG_DEBUG_LIST is enabled. Let's remove for_each_netdev() in gtp_net_exit_batch_rtnl() and delegate the destruction to default_device_exit_batch() as done in bareudp. [0]: list_del corruption, ffff8880aaa62c00->next (autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00/0x1000 [slab object]) is LIST_POISON1 (ffffffffffffff02) (prev is 0xffffffffffffff04) kernel BUG at lib/list_debug.c:58! Oops: invalid opcode: 0000 [#1] PREEMPT SMP KASAN CPU: 1 UID: 0 PID: 1804 Comm: kworker/u8:7 Tainted: G T 6.12.13-		

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
			grsec-full-20250211091339 #1 Tainted: [T]=RANDSTRUCT Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Workqueue: netns cleanup_net RIP: 0010:[<ffffffff84947381>] __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 Code: c2 76 91 31 c0 e8 9f b1 f7 fc 0f 0b 4d 89 f0 48 c7 c1 02 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 e0 c2 76 91 31 c0 e8 7f b1 f7 fc <0f> 0b 4d 89 e8 48 c7 c1 04 ff ff ff 48 89 ea 48 89 ee 48 c7 c7 60 RSP: 0018:fffffe8040b4fbd0 EFLAGS: 00010283 RAX: 00000000000000cc RBX: dffffc0000000000 RCX: ffffffff818c4054 RDX: ffffffff84947381 RSI: ffffffff818d1512 RDI: 0000000000000000 RBP: ffff8880aaa62c00 R08: 0000000000000001 R09: fffffbd008169f32 R10: fffffe8040b4f997 R11: 0000000000000001 R12: a1988d84f24943e4 R13: ffffffffffffff02 R14: ffffffffffffff04 R15: ffff8880aaa62c08 RBX: kasan shadow of 0x0 RCX: __wake_up_klogd.part.0+0x74/0xe0 kernel/printk/printk.c:4554 RDX: __list_del_entry_valid_or_report+0x141/0x200 lib/list_debug.c:58 RSI: vprintk+0x72/0x100 kernel/printk/printk_safe.c:71 RBP:		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc00 /0x1000 [slab object] RSP: process kstack ffffffe8040b4fbd0+0x7bd0/ 0x8000 [kworker/u8:7+netns 1804] R09: kasan shadow of process kstack ffffffe8040b4f990+0x7990/ 0x8000 [kworker/u8:7+netns 1804] R10: process kstack ffffffe8040b4f997+0x7997/ 0x8000 [kworker/u8:7+netns 1804] R15: autoslab_size_M_dev_P_net_core_dev_11127_8_1328_8_S_4096_A_64_n_139+0xc08 /0x1000 [slab object] FS: 0000000000000000(0000) GS:ffff888116000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000748f5372c000 CR3: 0000000015408000 CR4: 00000000003406f0 shadow CR4: 00000000003406f0 Stack: 0000000000000000 ffffffff8a0c35e7 ffffffff8a0c3603 ffff8880aaa62c00 ffff8880aaa62c00 0000000000000004 ffff88811145311c 0000000000000005 0000000000000001 ffff8880aaa62000 ffffffe8040b4fd40 ffffffff8a0c360d Call Trace: <TASK>		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff8a0c360d>] __list_del_entry_valid include/linux/list.h:131 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] __list_del_entry include/linux/list.h:248 [inline] fffffe8040b4fc28 [<ffffffff8a0c360d>] list_del include/linux/list.h:262 [inl ---truncated--- **CVE ID: CVE-2025-21865**		
Affected Version(s): From (including) 6.6.8 Up to (excluding) 6.6.80					
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2552
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.17					
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ibmvnic: Don't reference skb after sending to VIOS Previously, after successfully flushing the xmit buffer to VIOS, the tx_bytes stat was incremented by the length of the skb. It is invalid to access the skb memory after sending the buffer to	https://git.kernel.org/stable/c/093b0e5c90592773863f300b908b741622eef597, https://git.kernel.org/stable/c/25dddd01dcc8ef3acff964dbb32eeb0d89f098e9, https://git.kernel.org/stable/c/501ac6a7e21b82e05207c6b4449812d82820f306	O-LIN-LINU-180325/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the VIOS because, at any point after sending, the VIOS can trigger an interrupt to free this memory. A race between reading skb->len and freeing the skb is possible (especially during LPM) and will result in use-after-free: ========== ========== ========== === BUG: KASAN: slab-use-after-free in ibmvnic_xmit+0x75c/0x1808 [ibmvnic] Read of size 4 at addr c00000024eb48a70 by task hxecom/14495 <...> Call Trace: [c000000118f66cf0] [c0000000018cba6c] dump_stack_lvl+0x84/0xe8 (unreliable) [c000000118f66d20] [c0000000006f0080] print_report+0x1a8/0x7f0 [c000000118f66df0] [c0000000006f08f0] kasan_report+0x128/0x1f8 [c000000118f66f00] [c0000000006f2868] __asan_load4+0xac/0xe0 [c000000118f66f20] [c0080000046eac84] ibmvnic_xmit+0x75c/0x1808 [ibmvnic] [c000000118f67340] [c0000000014be168] dev_hard_start_xmit+0x150/0x358 <...> Freed by task 0: kasan_save_stack+0x34/0x68 kasan_save_track+0x2c/0x5		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 kasan_save_free_info+0x64/0x108 __kasan_mempool_poison_object+0x148/0x2d4 napi_skb_cache_put+0x5c/0x194 net_tx_action+0x154/0x5b8 handle_softirqs+0x20c/0x60c do_softirq_own_stack+0x6c/0x88 <...> The buggy address belongs to the object at c00000024eb48a00 which belongs to the cache skbuff_head_cache of size 224 ========== ========== ========== === **CVE ID: CVE-2025-21855**		
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: s390/ism: add release function for struct device According to device_release() in /drivers/base/core.c, a device without a release function is a broken device and must be fixed. The current code directly frees the device after calling device_add() without waiting for other kernel parts to release their references.	https://git.kernel.org/stable/c/0505ff2936f166405d81d0d454a81d9c14124344, https://git.kernel.org/stable/c/915e34d5ad35a6a9e56113f852ade4a730fb88f0, https://git.kernel.org/stable/c/940d15254d2216b585558bcf36312da50074e711	O-LIN-LINU-180325/2554

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thus, a reference could still be held to a struct device, e.g., by sysfs, leading to potential use-after-free issues if a proper release function is not set. **CVE ID: CVE-2025-21856**		
Use After Free	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: geneve: Fix use-after-free in geneve_find_dev(). syzkaller reported a use-after-free in geneve_find_dev() [0] without repro. geneve_configure() links struct geneve_dev.next to net_generic(net, geneve_net_id)->geneve_list. The net here could differ from dev_net(dev) if IFLA_NET_NS_PID, IFLA_NET_NS_FD, or IFLA_TARGET_NETNSID is set. When dev_net(dev) is dismantled, geneve_exit_batch_rtnl() finally calls unregister_netdevice_queue() for each dev in the netns, and later the dev is freed. However, its geneve_dev.next is still linked to the backend UDP socket netns. Then, use-after-free will occur when another geneve dev is created in the netns.	https://git.kernel.org/stable/c/3ce92ca990cfac88a87c61df3cc0b5880e688ecf, https://git.kernel.org/stable/c/5a0538ac6826807d6919f6aecbb8996c2865af2c, https://git.kernel.org/stable/c/788dbca056a8783ec063da3c9d49a3a71c76c283	O-LIN-LINU-180325/2555

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Let's call geneve_dellink() instead in geneve_destroy_tunnels(). [0]: BUG: KASAN: slab-use-after-free in geneve_find_dev drivers/net/geneve.c:1295 [inline] BUG: KASAN: slab-use-after-free in geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 Read of size 2 at addr ffff000054d6ee24 by task syz.1.4029/13441 CPU: 1 UID: 0 PID: 13441 Comm: syz.1.4029 Not tainted 6.13.0-g0ad9617c78ac #24 dc35ca22c79fb82e8e7bc5c9c9adafea898b1e3d Hardware name: linux,dummy-virt (DT) Call trace: show_stack+0x38/0x50 arch/arm64/kernel/stacktrace.c:466 (C) __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xbc/0x108 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0x16c/0x6f0 mm/kasan/report.c:489 kasan_report+0xc0/0x120 mm/kasan/report.c:602 __asan_report_load2_noabort+0x20/0x30 mm/kasan/report_generic.c:379 geneve_find_dev drivers/net/geneve.c:1295 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			geneve_configure+0x234/0x858 drivers/net/geneve.c:1343 geneve_newlink+0xb8/0x128 drivers/net/geneve.c:1634 rtnl_newlink_create+0x23c/0x868 net/core/rtnetlink.c:3795 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x618/0x838 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x5fc/0x8b0 net/netlink/af_netlink.c:1892 sock_sendmsg_nosec net/socket.c:713 [inline] __sock_sendmsg net/socket.c:728 [inline] ___sys_sendmsg+0x410/0x6f8 net/socket.c:2568 __sys_sendmsg+0x178/0x1d8 net/socket.c:2622		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__sys_sendmsg net/socket.c:2654 [inline] __do_sys_sendmsg net/socket.c:2659 [inline] __se_sys_sendmsg net/socket.c:2657 [inline] __arm64_sys_sendmsg+0x12c/0x1c8 net/socket.c:2657 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x90/0x278 arch/arm64/kernel/syscall.c:49 el0_svc_common+0x13c/0x250 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x54/0x70 arch/arm64/kernel/syscall.c:151 el0_svc+0x4c/0xa8 arch/arm64/kernel/entry-common.c:744 el0t_64_sync_handler+0x78/0x108 arch/arm64/kernel/entry-common.c:762 el0t_64_sync+0x198/0x1a0 arch/arm64/kernel/entry.S:600 Allocated by task 13247: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x30/0x68 mm/kasan/common.c:68 kasan_save_alloc_info+0x44/0x58 mm/kasan/generic.c:568 poison_kmalloc_redzone mm/kasan/common.c:377 [inline]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__kasan_kmalloc+0x84/0xa0 mm/kasan/common.c:394 kasan_kmalloc include/linux/kasan.h:260 [inline] __do_kmalloc_node mm/slub.c:4298 [inline] __kmalloc_node_noprof+0x2a0/0x560 mm/slub.c:4304 __kvmalloc_node_noprof+0x9c/0x230 mm/util.c:645 alloc_netdev_mqs+0xb8/0x11a0 net/core/dev.c:11470 rtnl_create_link+0x2b8/0xb50 net/core/rtnetlink.c:3604 rtnl_newlink_create+0x19c/0x868 net/core/rtnetlink.c:3780 __rtnl_newlink net/core/rtnetlink.c:3906 [inline] rtnl_newlink+0x1054/0x1630 net/core/rtnetlink.c:4021 rtnetlink_rcv_msg+0x61c/0x918 net/core/rtnetlink.c:6911 netlink_rcv_skb+0x1dc/0x398 net/netlink/af_netlink.c:2543 rtnetlink_rcv+0x34/0x50 net/core/rtnetlink.c:6938 netlink_unicast_kernel net/netlink/af_n ---truncated--- **CVE ID: CVE-2025-21858**		
N/A	12-Mar-2025	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/1e988c3fe1264	O-LIN-LINU-180325/2556

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			io_uring: prevent opcode speculation sqe->opcode is used for different tables, make sure we santitise it against speculations. **CVE ID: CVE-2025-21863**	708f4f92109203ac5b1d65de50b, https://git.kernel.org/stable/c/506b9b5e8c2d2a411ea8fe361333f5081c56d23a, https://git.kernel.org/stable/c/b9826e3b26ec031e9063f64a7c735449c43955e4	
Use of Uninitialized Resource	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drop_monitor: fix incorrect initialization order Syzkaller reports the following bug: BUG: spinlock bad magic on CPU#1, syz-executor.0/7995 lock: 0xffff88805303f3e0, .magic: 00000000, .owner: <none>/-1, .owner_cpu: 0 CPU: 1 PID: 7995 Comm: syz-executor.0 Tainted: G E 5.10.209+ #1 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0x119/0x179 lib/dump_stack.c:118 debug_spin_lock_before kernel/locking/spinlock_debug.c:83 [inline] do_raw_spin_lock+0x1f6/0x270 kernel/locking/spinlock_debug.c:112	https://git.kernel.org/stable/c/07b598c0e6f06a0f254c88dafb4ad50f8a8c6eea, https://git.kernel.org/stable/c/0efa6c42f81c60d8f72ba7f5ed8d4fec8c526282, https://git.kernel.org/stable/c/219a47d0e6195bd202f22855e35f25bd15bc4d58	O-LIN-LINU-180325/2557

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__raw_spin_lock_irqsave include/linux/spinlock_api_smp.h:117 [inline] _raw_spin_lock_irqsave+0x50/0x70 kernel/locking/spinlock.c:159 reset_per_cpu_data+0xe6/0x240 [drop_monitor] net_dm_cmd_trace+0x43d/0x17a0 [drop_monitor] genl_family_rcv_msg_doit+0x22f/0x330 net/netlink/genetlink.c:739 genl_family_rcv_msg net/netlink/genetlink.c:783 [inline] genl_rcv_msg+0x341/0x5a0 net/netlink/genetlink.c:800 netlink_rcv_skb+0x14d/0x440 net/netlink/af_netlink.c:2497 genl_rcv+0x29/0x40 net/netlink/genetlink.c:811 netlink_unicast_kernel net/netlink/af_netlink.c:1322 [inline] netlink_unicast+0x54b/0x800 net/netlink/af_netlink.c:1348 netlink_sendmsg+0x914/0xe00 net/netlink/af_netlink.c:1916 sock_sendmsg_nosec net/socket.c:651 [inline] __sock_sendmsg+0x157/0x190 net/socket.c:663 ___sys_sendmsg+0x712/0x870 net/socket.c:2378		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			___sys_sendmsg+0xf8/0x170 net/socket.c:2432 __sys_sendmsg+0xea/0x1b0 net/socket.c:2461 do_syscall_64+0x30/0x40 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x62/0xc7 RIP: 0033:0x7f3f9815aee9 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f3f972bf0c8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f3f9826d050 RCX: 00007f3f9815aee9 RDX: 0000000020000000 RSI: 0000000020001300 RDI: 0000000000000007 RBP: 00007f3f981b63bd R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000006e R14: 00007f3f9826d050 R15: 00007ffe01ee6768 If drop_monitor is built as a kernel module, syzkaller may have time to send a netlink NET_DM_CMD_START message during the module loading. This will call the net_dm_monitor_start() function that uses a spinlock that has not yet		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been initialized. To fix this, let's place resource initialization above the registration of a generic netlink family. Found by InfoTeCS on behalf of Linux Verification Center (linuxtesting.org) with Syzkaller. **CVE ID: CVE-2025-21862**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tcp: drop secpath at the same time as we currently drop dst Xiumei reported hitting the WARN in xfrm6_tunnel_net_exit while running tests that boil down to: - create a pair of netns - run a basic TCP test over ipcomp6 - delete the pair of netns The xfrm_state found on spi_byaddr was not deleted at the time we delete the netns, because we still have a reference on it. This lingering reference comes from a secpath (which holds a ref on the xfrm_state), which is still attached to an skb. This skb is not leaked, it ends up on sk_receive_queue and then gets defer-free'd by skb_attempt_defer_free. The problem happens when we defer freeing an skb (push it on one CPU's	https://git.kernel.org/stable/c/69cafd9413084cd5012cf5d7c7ec6f3d493726d9, https://git.kernel.org/stable/c/87858bbf21da239ace300d61dd209907995c0491, https://git.kernel.org/stable/c/9b6412e6979f6f9e0632075f8f008937b5cd4efd	O-LIN-LINU-180325/2558

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			defer_list), and don't flush that list before the netns is deleted. In that case, we still have a reference on the xfrm_state that we don't expect at this point. We already drop the skb's dst in the TCP receive path when it's no longer needed, so let's also drop the secpath. At this point, tcp_filter has already called into the LSM hooks that may require the secpath, so it should not be needed anymore. However, in some of those places, the MPTCP extension has just been attached to the skb, so we cannot simply drop all extensions. **CVE ID: CVE-2025-21864**		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: f_midi: f_midi_complete to call queue_work When using USB MIDI, a lock is attempted to be acquired twice through a re-entrant call to f_midi_transmit, causing a deadlock. Fix it by using queue_work() to schedule the inner f_midi_transmit() via a high priority work queue from the completion handler. **CVE ID: CVE-2025-21859**	https://git.kernel.org/stable/c/1f10923404705a94891e612dff3b75e828a78368, https://git.kernel.org/stable/c/24a942610ee9bafb2692a456ae850c5b2e409b05, https://git.kernel.org/stable/c/4ab37fcb42832cdd3e9d5e50653285ca84d6686f	O-LIN-LINU-180325/2559

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/code-patching: Fix KASAN hit by not flagging text patching area as VM_ALLOC Erhard reported the following KASAN hit while booting his PowerMac G4 with a KASAN-enabled kernel 6.13-rc6: BUG: KASAN: vmalloc-out-of-bounds in copy_to_kernel_nofault+0xd8/0x1c8 Write of size 8 at addr f1000000 by task chronyd/1293 CPU: 0 UID: 123 PID: 1293 Comm: chronyd Tainted: G W 6.13.0-rc6-PMacG4 #2 Tainted: [W]=WARN Hardware name: PowerMac3,6 7455 0x80010303 PowerMac Call Trace: [c2437590] [c1631a84] dump_stack_lvl+0x70/0x8c (unreliable) [c24375b0] [c0504998] print_report+0xdc/0x504 [c2437610] [c050475c] kasan_report+0xf8/0x108 [c2437690] [c0505a3c] kasan_check_range+0x24/0x18c [c24376a0] [c03fb5e4] copy_to_kernel_nofault+0xd8/0x1c8 [c24376c0] [c004c014] patch_instructions+0x15c/0x16c [c2437710] [c00731a8] bpf_arch_text_copy+0x60/0x7c [c2437730] [c0281168]	https://git.kernel.org/stable/c/2d542f13d26344e3452eee77613026ce9b653065, https://git.kernel.org/stable/c/2e6c80423f201405fd65254e52decd21663896f3, https://git.kernel.org/stable/c/6847b3e40bb963e57b61d1cc6fe84cb37b9d3d4c	O-LIN-LINU-180325/2560

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf_jit_binary_pack_finalize +0x50/0xac [c2437750] [c0073cf4] bpf_int_jit_compile+0xb30/ 0xdec [c2437880] [c0280394] bpf_prog_select_runtime+0x 15c/0x478 [c24378d0] [c1263428] bpf_prepare_filter+0xbf8/0 xc14 [c2437990] [c12677ec] bpf_prog_create_from_user+ 0x258/0x2b4 [c24379d0] [c027111c] do_seccomp+0x3dc/0x1890 [c2437ac0] [c001d8e0] system_call_exception+0x2d c/0x420 [c2437f30] [c00281ac] ret_from_syscall+0x0/0x2c --- interrupt: c00 at 0x5a1274 NIP: 005a1274 LR: 006a3b3c CTR: 005296c8 REGS: c2437f40 TRAP: 0c00 Tainted: G W (6.13.0-rc6-PMacG4) MSR: 0200f932 <VEC,EE,PR,FP,ME,IR,DR,RI > CR: 24004422 XER: 00000000 GPR00: 00000166 af8f3fa0 a7ee3540 00000001 00000000 013b6500 005a5858 0200f932 GPR08: 00000000 00001fe9 013d5fc8 005296c8 2822244c 00b2fcd8 00000000 af8f4b57 GPR16: 00000000 00000001 00000000 00000000 00000000 00000001 00000000 00000002 GPR24: 00afdbb0 00000000 00000000 00000000 006e0004 013ce060 006e7c1c 00000001		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NIP [005a1274] 0x5a1274 LR [006a3b3c] 0x6a3b3c --- interrupt: c00 The buggy address belongs to the virtual mapping at [f1000000, f1002000) created by: text_area_cpu_up+0x20/0x190 The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:00000000 index:0x0 pfn:0x76e30 flags: 0x80000000(zone=2) raw: 80000000 00000000 00000122 00000000 00000000 00000000 ffffffff 00000001 raw: 00000000 page dumped because: kasan: bad access detected Memory state around the buggy address: f0ffff00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0ffff80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >f1000000: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ f1000080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f1000100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ========== f8 corresponds to KASAN_VMALLOC_INVALID which means the area is not		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			initialised hence not supposed to be used yet. Powerpc text patching infrastructure allocates a virtual memory area using get_vm_area() and flags it as VM_ALLOC. But that flag is meant to be used for vmalloc() and vmalloc() allocated memory is not supposed to be used before a call to __vmalloc_node_range() which is never called for that area. That went undetected until commit e4137f08816b ("mm, kasan, kmsan: instrument copy_from/to_kernel_nofault") The area allocated by text_area_cpu_up() is not vmalloc memory, it is mapped directly on demand when needed by map_kernel_page(). There is no VM flag corresponding to such usage, so just pass no flag. That way the area will be unpoisonned and usable immediately. **CVE ID: CVE-2025-21866**		
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix deadlock when freeing cgroup storage The following commit bc235cdb423a ("bpf: Prevent deadlock from recursive bpf_task_storage_[get|delete	https://git.kernel.org/stable/c/6ecb9fa14eec5f15d97c84c36896871335f6ddfb, https://git.kernel.org/stable/c/c78f4afbd962f43a3989f45f3ca04300252b19b5, https://git.kernel.org/stable/c/f	O-LIN-LINU-180325/2561

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			]") first introduced deadlock prevention for fentry/fexit programs attaching on bpf_task_storage helpers. That commit also employed the logic in map free path in its v6 version. Later bpf_cgrp_storage was first introduced in c4bcfb38a95e ("bpf: Implement cgroup storage available to non-cgroup-attached bpf progs") which faces the same issue as bpf_task_storage, instead of its busy counter, NULL was passed to bpf_local_storage_map_free() which opened a window to cause deadlock: <TASK> (acquiring local_storage->lock) _raw_spin_lock_irqsave+0x3d/0x50 bpf_local_storage_update+0xd1/0x460 bpf_cgrp_storage_get+0x109/0x130 bpf_prog_a4d4a370ba857314_cgrp_ptr+0x139/0x170 ? __bpf_prog_enter_recur+0x16/0x80 bpf_trampoline_6442485186+0x43/0xa4 cgroup_storage_ptr+0x9/0x20 (holding local_storage->lock) bpf_selem_unlink_storage_nolock.constprop.0+0x135/0x160 bpf_selem_unlink_storage+0x6f/0x110 bpf_local_storage_map_free+0xa2/0x110 bpf_map_free_deferr	ac674d2bd68f3479f27328626b42d1eebd11fef	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ed+0x5b/0x90 process_one_work+0x17c/0x390 worker_thread+0x251/0x360 kthread+0xd2/0x100 ret_from_fork+0x34/0x50 ret_from_fork_asm+0x1a/0x30 </TASK> Progs: - A: SEC("fentry/cgroup_storage_ptr") - cgid (BPF_MAP_TYPE_HASH) Record the id of the cgroup the current task belonging to in this hash map, using the address of the cgroup as the map key. - cgrpa (BPF_MAP_TYPE_CGRP_STORAGE) If current task is a kworker, lookup the above hash map using function parameter @owner as the key to get its corresponding cgroup id which is then used to get a trusted pointer to the cgroup through bpf_cgroup_from_id(). This trusted pointer can then be passed to bpf_cgrp_storage_get() to finally trigger the deadlock issue. - B: SEC("tp_btf/sys_enter") - cgrpb (BPF_MAP_TYPE_CGRP_STORAGE) The only purpose of		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 prog is to fill Prog A's hash map by calling bpf_cgrp_storage_get() for as many userspace tasks as possible. Steps to reproduce: - Run A; - while (true) { Run B; Destroy B; } Fix this issue by passing its busy counter to the free procedure so it can be properly incremented before storage/smap locking. **CVE ID: CVE-2024-58088**		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: smb: client: Add check for next_buffer in receive_encrypted_standard () Add check for the return value of cifs_buf_get() and cifs_small_buf_get() in receive_encrypted_standard () to prevent null pointer dereference. **CVE ID: CVE-2025-21844**	https://git.kernel.org/stable/c/24e8e4523d3071bc5143b0db9127d511489f7b3b, https://git.kernel.org/stable/c/554736b583f529ee159aa95af9a0cbc12b5ffc96, https://git.kernel.org/stable/c/860ca5e50f73c2a1cef7eefc9d39d04e275417f7	O-LIN-LINU-180325/2562
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: acct: perform last write from workqueue In [1] it was reported that the acct(2) system call can be used to trigger NULL deref in cases where it is set to write to a file that	https://git.kernel.org/stable/c/56d5f3eba3f5de0efdd556de4ef381e109b973a9, https://git.kernel.org/stable/c/5a59ced8ffc71973d42c82484a719c8f6ac8f7f7, https://git.kernel.org/stable/c/5c928e14a2ccd	O-LIN-LINU-180325/2563

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			triggers an internal lookup. This can e.g., happen when pointing acc(2) to /sys/power/resume. At the point the where the write to this file happens the calling task has already exited and called exit_fs(). A lookup will thus trigger a NULL-deref when accessing current->fs. Reorganize the code so that the the final write happens from the workqueue but with the caller's credentials. This preserves the (strange) permission model and has almost no regression risk. This api should stop to exist though. **CVE ID: CVE-2025-21846**	99462f2351ead627b58075bb736	
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: sockmap, vsock: For connectible sockets allow only connected sockmap expects all vsocks to have a transport assigned, which is expressed in vsock_proto::psock_update_sk_prot(). However, there is an edge case where an unconnected (connectible) socket may lose its previously assigned transport. This is handled with a NULL check in the vsock/BPF recv path. Another design detail is that listening vsocks are not	https://git.kernel.org/stable/c/22b683217ad2112791a708693cb236507abd637a, https://git.kernel.org/stable/c/8fb5bb169d17cdd12c2dcc2e96830ed487d77a0f, https://git.kernel.org/stable/c/cc9a7832ede53ade1ba9991f0e27314caa4029d8	O-LIN-LINU-180325/2564

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			supposed to have any transport assigned at all. Which implies they are not supported by the sockmap. But this is complicated by the fact that a socket, before switching to TCP_LISTEN, may have had some transport assigned during a failed connect() attempt. Hence, we may end up with a listening vsock in a sockmap, which blows up quickly: KASAN: null-ptr-deref in range [0x0000000000000120-0x0000000000000127] CPU: 7 UID: 0 PID: 56 Comm: kworker/7:0 Not tainted 6.14.0-rc1+ Workqueue: vsock-loopback vsock_loopback_work RIP: 0010:vsock_read_skb+0x4b/0x90 Call Trace: sk_psock_verdict_data_ready+0xa4/0x2e0 virtio_transport_recv_pkt+0x1ca8/0x2acc vsock_loopback_work+0x27d/0x3f0 process_one_work+0x846/0x1420 worker_thread+0x5b3/0xf80 kthread+0x35a/0x700 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x1a/0x30 For connectible sockets, instead of relying solely on		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 state of vsk->transport, tell sockmap to only allow those representing established connections. This aligns with the behaviour for AF_INET and AF_UNIX. **CVE ID: CVE-2025-21854**		
N/A	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: avoid holding freeze_mutex during mmap operation We use map->freeze_mutex to prevent races between map_freeze() and memory mapping BPF map contents with writable permissions. The way we naively do this means we'll hold freeze_mutex for entire duration of all the mm and VMA manipulations, which is completely unnecessary. This can potentially also lead to deadlocks, as reported by syzbot in [0]. So, instead, hold freeze_mutex only during writeability checks, bump (proactively) "write active" count for the map, unlock the mutex and proceed with mmap logic. And only if something went wrong during mmap logic, then undo that "write active" counter increment. [0] https://lore.kernel.org/bpf/678dcbc9.050a0220.303755.0066.GAE@google.com/	https://git.kernel.org/stable/c/271e49f8a58edba65bc2b1250a0abaa98c4bfdbe, https://git.kernel.org/stable/c/29cfda62ab4d92ab94123813db49ab76c1e61b29, https://git.kernel.org/stable/c/bc27c52eea189e8f7492d40739b7746d67b65bbb	O-LIN-LINU-180325/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21853		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: fix error handling causing NULL dereference tcf_exts_miss_cookie_base_alloc() calls xa_alloc_cyclic() which can return 1 if the allocation succeeded after wrapping. This was treated as an error, with value 1 returned to caller tcf_exts_init_ex() which sets exts->actions to NULL and returns 1 to caller fl_change(). fl_change() treats err == 1 as success, calling tcf_exts_validate_ex() which calls tcf_action_init() with exts->actions as argument, where it is dereferenced. Example trace: BUG: kernel NULL pointer dereference, address: 0000000000000000 CPU: 114 PID: 16151 Comm: handler114 Kdump: loaded Not tainted 5.14.0-503.16.1.el9_5.x86_64 #1 RIP: 0010:tcf_action_init+0x1f8/0x2c0 Call Trace: tcf_action_init+0x1f8/0x2c0 tcf_exts_validate_ex+0x175/0x190 fl_change+0x537/0x1120 [cls_flower]	https://git.kernel.org/stable/c/071ed42cff4fcdd89025d966d48eabef59913bf2, https://git.kernel.org/stable/c/3c74b5787caf59bb1e9c5fe0a360643a71eb1e8a, https://git.kernel.org/stable/c/3e4c56cf41876ef2a82f0877fe2a67648f8632b8	O-LIN-LINU-180325/2566

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21857		
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: stream-ipc: Check for cstream nullity in sof_ipc_msg_data() The nullity of sps->cstream should be checked similarly as it is done in sof_set_stream_data_offset() function. Assuming that it is not NULL if sps->stream is NULL is incorrect and can lead to NULL pointer dereference. **CVE ID: CVE-2025-21847**	https://git.kernel.org/stable/c/2b3878baf90918a361a3dfd3513025100b1b40b6, https://git.kernel.org/stable/c/62ab1ae5511c59b5f0bf550136ff321331adca9f, https://git.kernel.org/stable/c/6c18f5eb2043ebf4674c08a9690218dc818a11ab	O-LIN-LINU-180325/2567
NULL Pointer Dereference	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfp: bpf: Add check for nfp_app_ctrl_msg_alloc() Add check for the return value of nfp_app_ctrl_msg_alloc() in nfp_bpf_cmsg_alloc() to prevent null pointer dereference. **CVE ID: CVE-2025-21848**	https://git.kernel.org/stable/c/1358d8e07afdf21d49ca6f00c56048442977e00a, https://git.kernel.org/stable/c/29ccb1e4040da6ff02b7e64efaa2f8e6bf06020d, https://git.kernel.org/stable/c/878e7b11736e062514e58f3b445ff343e6705537	O-LIN-LINU-180325/2568
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.6					
Improper Locking	12-Mar-2025	8.1	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid racy issue with session expire.	https://git.kernel.org/stable/c/2107ab40629aeabbec369cf34b8cf0f288c3eb1b, https://git.kernel.org/stable/c/37a0e2b362b3150317fb6e2139de67b1e29ae5ff, https://git.kernel.org/stable/c/	O-LIN-LINU-180325/2569

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-58087	450a844c045ff0895d41b05a1cbe8febd1acfcfd	
Affected Version(s): From (including) 6.9 Up to (excluding) 6.12.17					
Improper Locking	12-Mar-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Use spin_lock_irqsave() in interruptible context spin_lock/unlock() functions used in interrupt contexts could result in a deadlock, as seen in GitLab issue #13399, which occurs when interrupt comes in while holding a lock. Try to remedy the problem by saving irq state before spin lock acquisition. v2: add irqs' state save/restore calls to all locks/unlocks in signal_irq_work() execution (Maciej) v3: use with spin_lock_irqsave() in guc_lrc_desc_unpin() instead of other lock/unlock calls and add Fixes and Cc tags (Tvrtko); change title and commit message (cherry picked from commit c088387ddd6482b40f21ccf23db1125e8fa4af7e) **CVE ID: CVE-2025-21849**	https://git.kernel.org/stable/c/2bf1f4c129db7a10920655b000f0292f1ee509c2, https://git.kernel.org/stable/c/47ae46ac5407646420e06b78e0dad331e56a4bb4, https://git.kernel.org/stable/c/e49477f7f78598295551d486ecc7f020d796432e	O-LIN-LINU-180325/2570
Improper Locking	12-Mar-2025	3.3	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/517e8a7835e8cfb398a0aeb0133	O-LIN-LINU-180325/2571

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bpf: Fix softlockup in arena_map_free on 64k page kernel On an aarch64 kernel with CONFIG_PAGE_SIZE_64KB=y, arena_htab tests cause a segmentation fault and soft lockup. The same failure is not observed with 4k pages on aarch64. It turns out arena_map_free() is calling apply_to_existing_page_range() with the address returned by bpf_arena_get_kern_vm_start(). If this address is not page-aligned the code ends up calling apply_to_pte_range() with that unaligned address causing soft lockup. Fix it by round up GUARD_SZ to PAGE_SIZE << 1 so that the division by 2 in bpf_arena_get_kern_vm_start() returns a page-aligned value. **CVE ID: CVE-2025-21851**	de50e31cae32b, https://git.kernel.org/stable/c/787d556a3de447e70964a4bdeba9196f62a62b1e, https://git.kernel.org/stable/c/c1f3f3892d4526f18aaeffdb6068ce861e793ee3	
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Improper Access Control	03-Mar-2025	8.5	There is an improper access control issue in ArcGIS Server versions 10.9.1 through 11.3 on Windows and Linux, which under unique circumstances, could potentially allow a remote, low privileged authenticated attacker to access secure services published a	https://www.esri.com/arcgis-blog/products/trust-arcgis/administration/arcgis-server-security-2025-update-1-patch/	O-MIC-WIND-180325/2572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			standalone (Unfederated) ArcGIS Server instance. If successful this compromise would have a high impact on Confidentiality, low impact on integrity and no impact to availability of the software. **CVE ID: CVE-2024-51954**		
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20947					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2573
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2574
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2575
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2576
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2577
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-180325/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclose information with a physical attack. **CVE ID: CVE-2025-24984**	lity/CVE-2025-24984	
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7876					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2579
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2580
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2581
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2582
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2583
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2584
Product: windows_10_1809					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 10.0.17763.7009					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2585
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2586
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2587
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2588
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2589
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.5608					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2590
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-180325/2591

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-24993	lity/CVE-2025-24993	
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2592
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2593
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2594
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.5608					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2595
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2596
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2597
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an	https://msrc.microsoft.com/upd	O-MIC-WIND-180325/2598

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	ate-guide/vulnerability/CVE-2025-24991	
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2599
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.5039					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2600
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2601
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2602
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2603
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2604

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.5039					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2605
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2606
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2607
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2608
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2609
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.3403					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2610
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an	https://msrc.microsoft.com/update-	O-MIC-WIND-180325/2611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	guide/vulnerability/CVE-2025-26633	
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2612
Affected Version(s): * Up to (excluding) 10.0.26100.3476					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2613
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2614
Product: windows_server_2008					
Affected Version(s): -					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2615
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2616
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2617

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-26633		
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2618
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2619
Affected Version(s): r2					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2620
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2621
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2622
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2623
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2624

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: windows_server_2012					
Affected Version(s): -					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2625
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2626
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2627
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2628
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2629
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2630
Affected Version(s): r2					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-180325/2631

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	lity/CVE-2025-24985	
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2632
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2633
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2634
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2635
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2636
Product: windows_server_2016					
Affected Version(s): -					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2637

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2638
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2639
Affected Version(s): * Up to (excluding) 10.0.14393.7876					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2640
Use After Free	11-Mar-2025	7	Use after free in Windows Win32 Kernel Subsystem allows an authorized attacker to elevate privileges locally. **CVE ID: CVE-2025-24983**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983	O-MIC-WIND-180325/2641
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2642
Product: windows_server_2019					
Affected Version(s): -					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2643
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-180325/2644

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass a security feature locally. **CVE ID: CVE-2025-26633**	lity/CVE-2025-26633	
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2645
Affected Version(s): * Up to (excluding) 10.0.17763.7009					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2646
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2647
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.3270					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2648
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2649
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2650

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 10.0.20348.3328					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2651
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2652
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1486					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2653
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2654
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2655
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2656
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-180325/2657

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclose information with a physical attack. **CVE ID: CVE-2025-24984**	lity/CVE-2025-24984	
Product: windows_server_2025					
Affected Version(s): * Up to (excluding) 10.0.26100.3403					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24993**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993	O-MIC-WIND-180325/2658
Improper Neutralization	11-Mar-2025	7	Improper neutralization in Microsoft Management Console allows an unauthorized attacker to bypass a security feature locally. **CVE ID: CVE-2025-26633**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633	O-MIC-WIND-180325/2659
Out-of-bounds Read	11-Mar-2025	5.5	Out-of-bounds read in Windows NTFS allows an authorized attacker to disclose information locally. **CVE ID: CVE-2025-24991**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991	O-MIC-WIND-180325/2660
Affected Version(s): * Up to (excluding) 10.0.26100.3476					
Heap-based Buffer Overflow	11-Mar-2025	7.8	Integer overflow or wraparound in Windows Fast FAT Driver allows an unauthorized attacker to execute code locally. **CVE ID: CVE-2025-24985**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985	O-MIC-WIND-180325/2661
Insertion of Sensitive Information into Log File	11-Mar-2025	4.6	Insertion of sensitive information into log file in Windows NTFS allows an unauthorized attacker to disclose information with a physical attack. **CVE ID: CVE-2025-24984**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984	O-MIC-WIND-180325/2662
Vendor: openatom					
Product: openharmony					
Affected Version(s): * Up to (including) 5.0.2					
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local	https://gitee.com/openharmon	O-OPE-OPEN-180325/2663

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-20021**	y/security/blob/master/zh/security-disclosure/2025/2025-03.md	
Affected Version(s): From (including) 4.1 Up to (including) 5.0.2					
Out-of-bounds Read	04-Mar-2025	5.5	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause information leak through out-of-bounds read. **CVE ID: CVE-2025-20042**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2664
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-20081**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2665
Integer Overflow or Wraparound	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through integer overflow. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-20024**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2666
Integer Overflow or Wraparound	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through integer overflow. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-0587**	N/A	O-OPE-OPEN-180325/2667
Missing Release of Memory after Effective Lifetime	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker case DOS through missing release of memory. **CVE ID: CVE-2025-20011**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2668

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 4.1.0 Up to (including) 5.0.2					
Insecure Storage of Sensitive Information	04-Mar-2025	5.5	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause information leak through out-of-bounds read bypass permission check. **CVE ID: CVE-2025-21098**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2669
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-20091**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2670
Out-of-bounds Write	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-24309**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2671
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-20626**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2672
NULL Pointer Dereference	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through through NULL pointer dereference.. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-21084**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2673

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-24301**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2674
Out-of-bounds Write	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-23420**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2675
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-23414**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2676
Use After Free	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through use after free. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-23409**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2677
Out-of-bounds Write	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-23240**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2678

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Write	04-Mar-2025	3.8	in OpenHarmony v5.0.2 and prior versions allow a local attacker arbitrary code execution in pre-installed apps through out-of-bounds write. This vulnerability can be exploited only in restricted scenarios. **CVE ID: CVE-2025-22835**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2679
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-21089**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2680
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-23418**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through buffer overflow. **CVE ID: CVE-2025-23234**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2682
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through buffer overflow. **CVE ID: CVE-2025-22897**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2683
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-22847**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2684
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-22841**	https://gitee.com/openharmony/security/blob/master/zh/security-	O-OPE-OPEN-180325/2685

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				disclosure/2025/2025-03.md	
NULL Pointer Dereference	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through NULL pointer dereference. **CVE ID: CVE-2025-22837**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2686
Out-of-bounds Read	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through out-of-bounds read. **CVE ID: CVE-2025-22443**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2687
NULL Pointer Dereference	04-Mar-2025	3.3	in OpenHarmony v5.0.2 and prior versions allow a local attacker cause DOS through NULL pointer dereference. **CVE ID: CVE-2025-21097**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-03.md	O-OPE-OPEN-180325/2688
Vendor: Qualcomm					
Product: 205_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-205_-180325/2689
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-205_-180325/2690
Product: 215_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-215_-180325/2691

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-215_-180325/2692
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-215_-180325/2693
Product: 315_5g_iot_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-315_-180325/2694
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-315_-180325/2695
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-315_-180325/2696
Product: 9205_lte_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-9205-180325/2697

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: apq8017_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-APQ8-180325/2698
Product: aqt1000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AQT1-180325/2699
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AQT1-180325/2700
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AQT1-180325/2701
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AQT1-180325/2702
Product: ar8031_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-AR80-180325/2703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-53014	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2704
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2705
Product: ar8035_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2706
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2707
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2708
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2709
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-AR80-180325/2710

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2711
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2712
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2713
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2714
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-AR80-180325/2715
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-C-V2-180325/2716
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-C-V2-180325/2717

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-C-V2-180325/2718
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-C-V2-180325/2719
Product: csr8811_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSR8-180325/2720
Product: csra6620_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2721
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2722
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-CSRA-180325/2723

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2724
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2725
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2726
Product: csra6640_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2727
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2728
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2729
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-CSRA-180325/2730

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2731
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRA-180325/2732
Product: csrb31024_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-CSRB-180325/2733
Product: fastconnect_6200_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2734
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2735
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2736

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2737
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2738
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2739
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2740
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2741
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2742
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-FAST-180325/2743

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2744
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2745
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2746
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2747
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2748
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2749
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-FAST-180325/2750

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2751
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2752
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2753
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2754
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2755
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2756
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel	https://docs.qualcomm.com/product/publicres	O-QUA-FAST-180325/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	ources/security bulletin/march-2025-bulletin.html	
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2758
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2759
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2760
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2761
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2762
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2763
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters	https://docs.qualcomm.com/product/publicres	O-QUA-FAST-180325/2764

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2765
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2766
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2767
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2768
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2769
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2770
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-FAST-180325/2771

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2772
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2773
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2774
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2775
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2776
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2777

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2778
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2779
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2780
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2781
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2782
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2783
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2784

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2785
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2787
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2788
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2789
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2790
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FAST-180325/2791
Product: flight_rb5_5g_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FLIG-180325/2792
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FLIG-180325/2793
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FLIG-180325/2794
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FLIG-180325/2795
Product: fsm10056_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FSM1-180325/2796
Product: fsm20055_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FSM2-180325/2797
Product: fsm20056_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-FSM2-180325/2798
Product: immersive_home_214_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2799
Product: immersive_home_216_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2800
Product: immersive_home_316_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2801
Product: immersive_home_318_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2802
Product: immersive_home_3210_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2803
Product: immersive_home_326_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IMME-180325/2804
Product: ipq5010_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2805
Product: ipq5028_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2806
Product: ipq5300_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2807
Product: ipq5302_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2808
Product: ipq5312_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2809
Product: ipq5332_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ5-180325/2810
Product: ipq6000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ6-180325/2811
Product: ipq6010_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ6-180325/2812
Product: ipq6018_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ6-180325/2813
Product: ipq6028_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ6-180325/2814
Product: ipq8070a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2815
Product: ipq8071a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2816
Product: ipq8072a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2817
Product: ipq8074a_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2818
Product: ipq8076a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2819
Product: ipq8076_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2820
Product: ipq8078a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2821
Product: ipq8078_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2822
Product: ipq8173_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2823
Product: ipq8174_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ8-180325/2824
Product: ipq9008_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ9-180325/2825
Product: ipq9048_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ9-180325/2826
Product: ipq9554_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ9-180325/2827
Product: ipq9570_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ9-180325/2828
Product: ipq9574_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-IPQ9-180325/2829
Product: mdm9205s_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2830
Product: mdm9628_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2831
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2832
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-MDM9-180325/2833

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2834
Product: mdm9640_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2835
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MDM9-180325/2836
Product: msm8996au_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MSM8-180325/2837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MSM8-180325/2838
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-MSM8-180325/2839

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: pmp8074_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-PMP8-180325/2840
Product: qam8255p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2841
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2842
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2843
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2844
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2845
Time-of-check Time-of-use	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual	https://docs.qualcomm.com/product/publicres	O-QUA-QAM8-180325/2846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			device due to guest VM interaction. **CVE ID: CVE-2024-53032**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2847
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2848
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2849
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2850
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2851
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2852
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAM8-180325/2853

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2854
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2855
Product: qam8295p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2856
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2857
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2858
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2859
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-180325/2860

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2861
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2862
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2863
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2864
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2865
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2866
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-180325/2867

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53030	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2868
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2869
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2870
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2871
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2872
Product: qam8620p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2873
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer	https://docs.qualcomm.com/product/publicres	O-QUA-QAM8-180325/2874

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	ources/security bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2875
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2876
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2877
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2878
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2879
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2880
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAM8-180325/2881

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53022	2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2882
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2884
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2885
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2886
Product: qam8650p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2887
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-180325/2888

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53031	bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2889
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2890
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2891
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2892
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2893
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2894
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAM8-180325/2895

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2896
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2898
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2899
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2900
Product: qam8775p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2901
Time-of-check Time-of-use (TOCTOU)	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-180325/2902

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			**CVE ID: CVE-2024-53028**	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2903
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2904
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2905
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2906
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2907
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2908
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAM8-180325/2909

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2910
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2911
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2913
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2914
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAM8-180325/2915
Product: qamsrv1h_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU)	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAMS-180325/2916

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			**CVE ID: CVE-2024-53032**	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2917
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2918
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2919
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2920
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2921
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2922
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAMS-180325/2923

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2924
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2925
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2927
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2928
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2929
Product: qamsrv1m_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAMS-180325/2930

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53030	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2931
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2932
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2933
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2934
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2935
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2936
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QAMS-180325/2937

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2938
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2939
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2941
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2942
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QAMS-180325/2943
Product: qca0000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA0-180325/2944

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Product: qca4004_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA4-180325/2945
Product: qca4024_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA4-180325/2946
Product: qca6174a_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2947
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2948
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2949
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/2950

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53023	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2951
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2952
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2953
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2954
Product: qca6175a_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2955
Product: qca6310_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2956

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2957
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2958
Product: qca6320_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2959
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2960
Product: qca6335_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2961
Product: qca6391_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2962

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2963
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2964
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2965
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2966
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2967
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2968
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2969

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2970
Product: qca6420_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2971
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2972
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2973
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2974
Product: qca6421_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2975
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-180325/2976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Product: qca6426_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2977
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2978
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2979
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2980
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2981
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2982
Product: qca6430_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2983
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2984
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2985
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2986
Product: qca6431_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2987
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2988
Product: qca6436_firmware					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2989
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2990
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2992
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2993
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2994
Product: qca6554a_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/2995

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Product: qca6564au_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2996
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2997
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/2999
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3000
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3001
Product: qca6564a_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3002
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3003
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3004
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3005
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3006
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3007
Product: qca6564_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3008

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3009
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3010
Product: qca6574au_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3011
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3012
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3013
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3014
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/3015

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3016
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3017
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3018
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3019
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3020
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3021
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3022

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3024
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3025
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3026
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3027
Product: qca6574a_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3028
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/3029

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3030
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3031
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3032
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3033
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3034
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3035
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3036

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3037
Product: qca6574_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3038
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3039
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3040
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3042
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/3043

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3044
Product: qca6584au_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3045
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3046
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3047
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3048
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3049
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-180325/3050

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3051
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3052
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3053
Product: qca6584_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3054
Product: qca6595au_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3055
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3056

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3057
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3058
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3059
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3060
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3061
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3062
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3063

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3064
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3066
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3067
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3068
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3069
Product: qca6595_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3070

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3071
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3072
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3073
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3074
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3075
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3076
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3077

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3078
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3079
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3080
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3081
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3082
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3083
Product: qca6678aq_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3084

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3085
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3086
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3087
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3089
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3090
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3091

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qca6688aq_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3092
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3093
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3094
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3095
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3096
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3097
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3098

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3099
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3100
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3101
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3102
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3103
Product: qca6696_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3104
Time-of-check Time-of-use (TOCTOU)	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/3105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			**CVE ID: CVE-2024-53028**	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3106
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3107
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3108
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3109
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3110
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3111
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3112

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3113
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3114
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3115
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3116
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3117
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3118
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3119

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3120
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3121
Product: qca6698aq_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3122
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3123
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3124
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3125
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-180325/3126

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53030	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3127
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3128
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3129
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3130
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3131
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3132
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3133

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3134
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3135
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3136
Product: qca6777aq_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3137
Product: qca6787aq_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3138
Product: qca6797aq_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA6-180325/3139

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3140
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3141
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3142
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3143
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3144
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3145
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA6-180325/3146

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qca8072_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3147
Product: qca8075_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3148
Product: qca8081_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3149
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3150
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3151
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3152

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3153
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3154
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3155
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3156
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3157
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3158
Product: qca8082_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA8-180325/3159

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: qca8084_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3160
Product: qca8085_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3161
Product: qca8337_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3162
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3163
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3164
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCA8-180325/3165

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3166
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3167
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3168
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3169
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3170
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA8-180325/3171
Product: qca8386_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA8-180325/3172

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	bulletin/march-2025-bulletin.html	
Product: qca9367_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3173
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3174
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3175
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3176
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3177
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3178
Product: qca9377_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3179
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3180
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3181
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3182
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3184
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3185

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3186
Product: qca9888_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3187
Product: qca9889_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCA9-180325/3188
Product: qcc2073_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC2-180325/3189
Product: qcc2076_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC2-180325/3190
Product: qcc710_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3191
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3192
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3193
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3194
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3196
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3197

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3198
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3199
Product: qcc711_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCC7-180325/3200
Product: qcf8000sfp_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCF8-180325/3201
Product: qcf8000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCF8-180325/3202
Product: qcf8001_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	O-QUA-QCF8-180325/3203

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Product: qcm2150_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3204
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3205
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3206
Product: qcm2290_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3207
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3208
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCM2-180325/3209

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3210
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM2-180325/3211
Product: qcm4290_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3212
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3214
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3215
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM4-180325/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure. **CVE ID: CVE-2024-38426**	bulletin/march-2025-bulletin.html	
Product: qcm4325_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3217
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3218
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3219
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3220
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3221
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3222
Product: qcm4490_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3223
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3224
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3225
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3226
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM4-180325/3227
Product: qcm5430_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM5-180325/3228
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCM5-180325/3229

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM5-180325/3230
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM5-180325/3231
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM5-180325/3232
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM5-180325/3233
Product: qcm6125_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3234
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3235
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-QCM6-180325/3236

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3237
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3238
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3239
Product: qcm6490_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3240
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3241
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3242

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3243
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3244
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM6-180325/3245
Product: qcm8550_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3246
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3247
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3248
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCM8-180325/3249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3250
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3251
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCM8-180325/3252
Product: qcn5021_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3253
Product: qcn5022_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3254
Product: qcn5024_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCN5-180325/3255

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: qcn5052_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3256
Product: qcn5054_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3257
Product: qcn5122_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3258
Product: qcn5124_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3259
Product: qcn5152_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCN5-180325/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: qcn5154_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3261
Product: qcn5164_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN5-180325/3262
Product: qcn6023_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3263
Product: qcn6024_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3264
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3265

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3266
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3267
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3268
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3269
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3270
Product: qcn6100_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3271
Product: qcn6102_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicres	O-QUA-QCN6-180325/3272

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43057	ources/security bulletin/march-2025-bulletin.html	
Product: qcn6112_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3273
Product: qcn6122_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3274
Product: qcn6132_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3275
Product: qcn6224_firmware					
Affected Version(s): -					
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3276
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3277

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3278
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3279
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3280
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3281
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3282
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3283
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3284
Product: qcn6274_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3285
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3286
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3287
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3288
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3290
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3291

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3292
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3293
Product: qcn6402_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3294
Product: qcn6412_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3295
Product: qcn6422_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN6-180325/3296
Product: qcn6432_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCN6-180325/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43057	bulletin/march-2025-bulletin.html	
Product: qcn7606_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN7-180325/3298
Product: qcn9000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3299
Product: qcn9011_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3300
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3301
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3302
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCN9-180325/3303

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Product: qcn9012_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3304
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3305
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3306
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3307
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3308
Product: qcn9022_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3309

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcn9024_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3310
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3311
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3312
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3313
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3314
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3315
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCN9-180325/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: qcn9070_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3317
Product: qcn9072_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3318
Product: qcn9074_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3319
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3320
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3321
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCN9-180325/3322

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Product: qcn9100_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3323
Product: qcn9160_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3324
Product: qcn9274_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3325
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3326
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3327
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCN9-180325/3328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCN9-180325/3329
Product: qcs2290_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS2-180325/3330
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS2-180325/3331
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS2-180325/3332
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS2-180325/3333
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS2-180325/3334
Product: qcs410_firmware					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3335
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3336
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3337
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3338
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3339
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3340
Product: qcs4290_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCS4-180325/3341

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3343
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3344
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3345
Product: qcs4490_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3346
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3347
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS4-180325/3348

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3349
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3350
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS4-180325/3351
Product: qcs5430_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS5-180325/3352
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS5-180325/3353
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS5-180325/3354
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	O-QUA-QCS5-180325/3355

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS5-180325/3356
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS5-180325/3357
Product: qcs610_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3358
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3359
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3360
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3361

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3362
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3363
Product: qcs6125_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3364
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3365
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3366
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3367
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCS6-180325/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3369
Product: qcs615_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3371
Product: qcs6490_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3372
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3373
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3374

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3375
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3376
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS6-180325/3377
Product: qcs7230_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS7-180325/3378
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS7-180325/3379
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS7-180325/3380
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QCS7-180325/3381

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS7-180325/3382
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS7-180325/3383
Product: qcs8155_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3384
Product: qcs8250_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3385
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3386
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3387

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3389
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3390
Product: qcs8300_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3391
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3392
Product: qcs8550_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3393
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a	https://docs.qualcomm.com/product/publicres	O-QUA-QCS8-180325/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			variable during extended back to back tests. **CVE ID: CVE-2024-53023**	ources/security bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3395
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3396
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3397
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3398
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3399
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS8-180325/3400
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCS8-180325/3401

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Product: qcs9100_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS9-180325/3402
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS9-180325/3403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS9-180325/3404
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS9-180325/3405
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QCS9-180325/3406
Product: qdu1000_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3407

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3408
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3409
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3410
Product: qdu1010_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3411
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3412
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3413
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QDU1-180325/3414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: qdu1110_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3415
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3416
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3417
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3418
Product: qdu1210_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3419
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3420

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3421
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDU1-180325/3422
Product: qdx1010_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3423
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3424
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3425
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3426
Product: qdx1011_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-QDX1-180325/3427

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3428
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3429
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QDX1-180325/3430
Product: qep8111_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3431
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3432
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3433

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3434
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3435
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3436
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QEP8-180325/3437
Product: qfw7114_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3438
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3439
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QFW7-180325/3440

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43060	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3441
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3442
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3443
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3444
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3445
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3446
Product: qfw7124_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QFW7-180325/3447

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3448
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3449
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3450
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3451
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3452
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3453
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QFW7-180325/3454

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QFW7-180325/3455
Product: qmp1000_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QMP1-180325/3456
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QMP1-180325/3457
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QMP1-180325/3458
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QMP1-180325/3459
Product: qrb5165m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3460

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3461
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3462
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3463
Product: qrb5165n_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3464
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3465
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRB5-180325/3466
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-QRB5-180325/3467

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Product: qru1032_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3468
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3469
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3470
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3471
Product: qru1052_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3472
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3473

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3474
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3475
Product: qru1062_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3476
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3477
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3478
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QRU1-180325/3479
Product: qsm8250_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-QSM8-180325/3480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3481
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3482
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3483
Product: qsm8350_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3484
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3485
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QSM8-180325/3486
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	O-QUA-QSM8-180325/3487

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Product: qts110_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QTS1-180325/3488
Product: qxm8083_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-QXM8-180325/3489
Product: robotics_rb2_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3490
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3491
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3493
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3494
Product: robotics_rb3_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3495
Product: robotics_rb5_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3496
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3497
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-ROBO-180325/3498
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	O-QUA-ROBO-180325/3499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Product: sa2150p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA21-180325/3500
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA21-180325/3501
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA21-180325/3502
Product: sa4150p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3503
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3504
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA41-180325/3505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3506
Product: sa4155p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3507
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3508
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3509
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA41-180325/3510
Product: sa6145p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3511

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3512
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3513
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3514
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3515
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3516
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3518

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3519
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3520
Product: sa6150p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3521
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3522
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3523
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3524
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA61-180325/3525

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43060	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3526
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3528
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3529
Product: sa6155p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3530
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3531
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-SA61-180325/3532

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3533
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3534
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3535
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3536
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3537
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3538
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA61-180325/3539

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3540
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3541
Product: sa6155_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3542
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3543
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3544
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3545
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	O-QUA-SA61-180325/3546

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3547
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA61-180325/3548
Product: sa7255p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3549
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3550
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3551
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3552

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3553
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3554
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3555
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3556
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3557
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3558
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3559

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3560
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3561
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA72-180325/3562
Product: sa7775p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3563
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3564
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3565
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA77-180325/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3567
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3568
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3569
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3570
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3571
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3572
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3573

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3574
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3575
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA77-180325/3576
Product: sa8145p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3577
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3578
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3579
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA81-180325/3580

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3581
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3582
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3584
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3585
Product: sa8150p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3586
Time-of-check Time-of-use	03-Mar-2025	7.8	Memory corruption may occur while processing	https://docs.qualcomm.com/product/publicres	O-QUA-SA81-180325/3587

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			message from frontend during allocation. **CVE ID: CVE-2024-53028**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3588
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3589
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3590
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3591
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3592
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3593
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA81-180325/3594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3595
Product: sa8155p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3596
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3597
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3598
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3599
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3600

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3601
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3602
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3603
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3605
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3606
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3607
Product: sa8155_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3608
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3609
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3610
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3611
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3612
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3613
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3614

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sa8195p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3615
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3616
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3617
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3618
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3619
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3620
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA81-180325/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3622
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3624
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA81-180325/3625
Product: sa8255p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3626
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3627
Time-of-check Time-of-use	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual	https://docs.qualcomm.com/product/publicres	O-QUA-SA82-180325/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
(TOCTOU) Race Condition			device due to guest VM interaction. **CVE ID: CVE-2024-53032**	ources/security bulletin/march-2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3629
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3630
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3631
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3632
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3633
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3634
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA82-180325/3635

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3636
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3637
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3638
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3639
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3640
Product: sa8295p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3641
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA82-180325/3642

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53029	bulletin/march-2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3643
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3644
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3645
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3646
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3647
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3648
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA82-180325/3649

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3650
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3651
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3652
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3653
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3654
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3655
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA82-180325/3656

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA82-180325/3657
Product: sa8530p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3658
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3659
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3660
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3661
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3662
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	O-QUA-SA85-180325/3663

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3664
Product: sa8540p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3665
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3666
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3667
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3668
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3669

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3670
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3671
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3672
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3673
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3674
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3675
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3676

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3677
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3678
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3679
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA85-180325/3680
Product: sa8620p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3681
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3682
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA86-180325/3683

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3684
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3685
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3686
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3687
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3688
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3689
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3690

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3692
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3693
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3694
Product: sa8650p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3695
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3696
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA86-180325/3697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3698
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3699
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3700
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3701
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3702
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3703
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3704

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3706
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3707
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA86-180325/3708
Product: sa8770p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3709
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3710
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA87-180325/3711

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3712
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3713
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3714
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3715
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3716
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3717
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3718

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3719
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3721
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3722
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3723
Product: sa8775p_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3724
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA87-180325/3725

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3726
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3727
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3728
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3729
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3730
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3731
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3732

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3733
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3734
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3735
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3736
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3737
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA87-180325/3738
Product: sa9000p_firmware					
Affected Version(s): -					
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SA90-180325/3739

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3740
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3741
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3742
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3743
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3744
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3745
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3746

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3747
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3748
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3749
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3750
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3751
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3752
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3753

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3754
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SA90-180325/3755
Product: sc8180x-aaab_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC81-180325/3756
Product: sc8180x-acaf_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC81-180325/3757
Product: sc8180x-ad_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC81-180325/3758
Product: sc8180xp-aaab_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SC81-180325/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43056	bulletin/march-2025-bulletin.html	
Product: sc8180xp-acaf_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC81-180325/3760
Product: sc8180xp-ad_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC81-180325/3761
Product: sc8280xp-abbb_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC82-180325/3762
Product: sc8380xp_firmware					
Affected Version(s): -					
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC83-180325/3763
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC83-180325/3764

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53034		
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC83-180325/3765
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SC83-180325/3766
Product: sd460_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD46-180325/3767
Product: sd660_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD66-180325/3768
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD66-180325/3769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD66-180325/3770

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sd662_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD66-180325/3771
Product: sd670_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3772
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3773
Product: sd675_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3774
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3775
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3776

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD67-180325/3777
Product: sd730_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD73-180325/3778
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD73-180325/3779
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD73-180325/3780
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD73-180325/3781
Product: sd835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD83-180325/3782
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicres	O-QUA-SD83-180325/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure. **CVE ID: CVE-2024-38426**	ources/security bulletin/march-2025-bulletin.html	
Product: sd855_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD85-180325/3784
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD85-180325/3785
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD85-180325/3786
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD85-180325/3787
Product: sd865_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD86-180325/3788
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SD86-180325/3789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD86-180325/3790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD86-180325/3791
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD86-180325/3792
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD86-180325/3793
Product: sd888_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD88-180325/3794
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD88-180325/3795
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SD88-180325/3796

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD88-180325/3797
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD88-180325/3798
Product: sdm429w_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3799
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3800
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3801
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3802

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3803
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3804
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3805
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3806
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3807
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3808
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3809

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3810
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3811
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDM4-180325/3812
Product: sdx55_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3813
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3814
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3815
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SDX5-180325/3816

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3817
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3818
Product: sdx57m_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3819
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX5-180325/3820
Product: sdx61_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3821
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3822

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3824
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3825
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3826
Product: sdx65m_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX6-180325/3827
Product: sdx71m_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX7-180325/3828
Product: sdx80m_firmware					
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
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX8-180325/3829
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SDX8-180325/3830
Product: sd_675_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_6-180325/3831
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_6-180325/3832
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_6-180325/3833
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_6-180325/3834
Product: sd_8cx_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/product/publicres	O-QUA-SD_8-180325/3835

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	ources/security bulletin/march-2025-bulletin.html	
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3836
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3837
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3838
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3839
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3840
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SD_8-180325/3841
Product: sg4150p_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3842
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3843
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3844
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3845
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3846
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3847
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG41-180325/3848

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sg8275p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3849
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3850
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3852
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3853
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SG82-180325/3854
Product: sm4125_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SM41-180325/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM41-180325/3856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM41-180325/3857
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM41-180325/3858
Product: sm4635_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3859
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3860
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3861

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3862
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3863
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM46-180325/3864
Product: sm6250_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM62-180325/3865
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM62-180325/3866
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM62-180325/3867
Product: sm6370_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-SM63-180325/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM63-180325/3869
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM63-180325/3870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM63-180325/3871
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM63-180325/3872
Product: sm6650_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3873
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3874

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3876
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3877
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3878
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM66-180325/3879
Product: sm7250p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM72-180325/3880
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SM72-180325/3881

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM72-180325/3882
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM72-180325/3883
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM72-180325/3884
Product: sm7315_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3885
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3886
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3887
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM73-180325/3888

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3889
Product: sm7325p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3890
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3891
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3893
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM73-180325/3894
Product: sm7635_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3895
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3896
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3898
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3899
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3900
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3901
Product: sm7675p_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3902
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3903
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3905
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3906
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3907
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3908

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: sm7675_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3909
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3910
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3912
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3913
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM76-180325/3914
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SM76-180325/3915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-38426	2025-bulletin.html	
Product: sm8550p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3916
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3917
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3918
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3919
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3920
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM85-180325/3921
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SM85-180325/3922

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Product: sm8635p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3923
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3924
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3925
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3926
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3927
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3928
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication	https://docs.qualcomm.com/product/publicres	O-QUA-SM86-180325/3929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may lead to information disclosure. **CVE ID: CVE-2024-38426**	ources/security bulletin/march-2025-bulletin.html	
Product: sm8635_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3930
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3931
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3932
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3933
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3934
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3935

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3936
Product: sm8650q_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3937
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3938
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3939
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3940
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3941
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SM86-180325/3942

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM86-180325/3943
Product: sm8735_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3944
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3945
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3946
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3947
Product: sm8750p_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3948

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3949
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3950
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3951
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3952
Product: sm8750_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3953
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3954
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SM87-180325/3955

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3956
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SM87-180325/3957
Product: smart_audio_400_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SMAR-180325/3958
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SMAR-180325/3959
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SMAR-180325/3960
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SMAR-180325/3961
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SMAR-180325/3962

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SMAR-180325/3963
Product: snapdragon_210_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3964
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3965
Product: snapdragon_212_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3966
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3967
Product: snapdragon_429_firmware					
Affected Version(s): -					
Buffer Copy without Checking	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call.	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/3968

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-43055**	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3969
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3970
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3971
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3972
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3973
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3974
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/3975

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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`s frame processing pipeline. **CVE ID: CVE-2024-49836**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3976
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3978
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3979
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3980
Product: snapdragon_429_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3981
Product: snapdragon_439_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3982
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3983
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3984
Product: snapdragon_460_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3985
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3986
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3987
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/3988

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3989
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3990
Product: snapdragon_460_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3991
Product: snapdragon_480\+_5g_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3992
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3993
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3994

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3995
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3996
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3997
Product: snapdragon_480_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3998
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/3999
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4000
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4002
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4003
Product: snapdragon_4_gen_1_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4004
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4005
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4007
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4008

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4009
Product: snapdragon_4_gen_2_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4010
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4011
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4012
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4013
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4014
Product: snapdragon_660_firmware					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4015
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4017
Product: snapdragon_662_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4018
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4019
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4020
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4022
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4023
Product: snapdragon_662_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4024
Product: snapdragon_665_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4025
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4026
Product: snapdragon_670_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4027

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4028
Product: snapdragon_675_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4029
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4030
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4031
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4032
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4033
Product: snapdragon_678_firmware					
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
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4034
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4035
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4036
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4037
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4038
Product: snapdragon_680_4g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4039
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4042
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4043
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4044
Product: snapdragon_680_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4045
Product: snapdragon_685_4g_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4046

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4047
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4049
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4050
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4051
Product: snapdragon_685_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4052
Product: snapdragon_690_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4053

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4054
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4055
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4056
Product: snapdragon_695_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4057
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4058
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4059

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4060
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4061
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4062
Product: snapdragon_710_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4063
Product: snapdragon_720g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4064
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4065
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Product: snapdragon_730g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4067
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4068
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4069
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4070
Product: snapdragon_730_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4071
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4072

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4073
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4074
Product: snapdragon_732g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4075
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4076
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4077
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4078
Product: snapdragon_750g_5g_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4079
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4080
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4081
Product: snapdragon_765g_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4082
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4083
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4084
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4085

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4086
Product: snapdragon_765_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4087
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4088
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4089
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4090
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4091
Product: snapdragon_768g_5g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4092
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4093
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4094
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4095
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4096
Product: snapdragon_778g\+_5g_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4097
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4098

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4100
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4101
Product: snapdragon_778g_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4102
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4103
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4104
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4106
Product: snapdragon_780g_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4107
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4108
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4109
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4110
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4111
Product: snapdragon_782g_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4112
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4113
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4115
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4116
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4117
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4118

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4120
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4121
Product: snapdragon_820_automotive_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4123
Product: snapdragon_835_mobile_pc_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4124

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_835_pc_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4125
Product: snapdragon_845_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4126
Product: snapdragon_850_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4127
Product: snapdragon_855\+_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4128
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4129
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4130

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4131
Product: snapdragon_855_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4132
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4133
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4134
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4135
Product: snapdragon_860_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4136

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4137
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4138
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4139
Product: snapdragon_8657+_5g_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4140
Product: snapdragon_865\+_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4141
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4142
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4143

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4144
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4145
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4146
Product: snapdragon_865_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4147
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4148
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4149

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4150
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4151
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4152
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4153
Product: snapdragon_870_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4154
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4155
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4157
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4158
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4159
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4160
Product: snapdragon_888\+_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4161
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4162
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4163

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4165
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4166
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4167
Product: snapdragon_888_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4168
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4169
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4170

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4171
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4172
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4173
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4174
Product: snapdragon_8cx_gen_3_compute_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4175
Product: snapdragon_8\+_gen_1_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4176

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4178
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4179
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4180
Product: snapdragon_8\+_gen_2_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4181
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4182
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4183

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4184
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4185
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4186
Product: snapdragon_8\+_gen_2_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4187
Product: snapdragon_8_gen_1_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4188
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4189

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4190
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4191
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4192
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4193
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4194
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4195
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4197
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4198
Product: snapdragon_8_gen_2_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4199
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4200
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4201
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4202
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4203

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4204
Product: snapdragon_8_gen_2_mobile_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4205
Product: snapdragon_8_gen_3_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4206
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4207
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4208
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4209

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4211
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4212
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4213
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4214
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4215
Product: snapdragon_ar1_gen_1_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4216

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4217
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4218
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4219
Product: snapdragon_ar1_gen_1__firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4220
Product: snapdragon_ar2_gen_1_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4221
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4222

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4223
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4224
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4225
Product: snapdragon_ar2_gen_1_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4226
Product: snapdragon_auto_4g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4227
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4228
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4229

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4230
Product: snapdragon_auto_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4231
Product: snapdragon_auto_5g-rf_gen_2_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4232
Product: snapdragon_auto_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4233
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4235
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4236
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4237
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4238
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4239
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4240
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4241

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4242
Product: snapdragon_w5\+_gen_1_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4243
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4244
Product: snapdragon_w5\+_gen_1_wearable_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4245
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4246
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4247

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4248
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4250
Product: snapdragon_wear_1300_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4251
Product: snapdragon_wear_4100\+_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4252
Product: snapdragon_wear_4100\+__firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4253

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_x12_lte_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4254
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4255
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4256
Product: snapdragon_x24_lte_firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4257
Product: snapdragon_x35_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4258
Product: snapdragon_x35_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4259

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4260
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4261
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4262
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4263
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4264
Product: snapdragon_x50_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4265

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4266
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4267
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4268
Product: snapdragon_x55_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4269
Product: snapdragon_x55_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4270
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4271
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-180325/4272

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	ources/security bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4273
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4274
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4275
Product: snapdragon_x5_lte_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4276
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4277
Product: snapdragon_x62_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: snapdragon_x62_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4279
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4280
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4282
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4283
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4284
Product: snapdragon_x65_5g-rf_firmware					
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
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4285
Product: snapdragon_x65_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4286
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4287
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4288
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4290
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4291

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4292
Product: snapdragon_x70-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4293
Product: snapdragon_x72_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4294
Product: snapdragon_x72_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4295
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4296
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SNAP-180325/4297

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4298
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4299
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4300
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4301
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4302
Product: snapdragon_x75_5g-rf_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4303
Product: snapdragon_x75_5g_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4304
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4305
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4306
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4307
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4309
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4310
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	O-QUA-SNAP-180325/4311

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Product: snapdragon_xr1_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4312
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4313
Product: snapdragon_xr2\+_gen_1_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4314
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4316
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SNAP-180325/4317

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4318
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4319
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4320
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4321
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4322
Product: snapdragon_xr2_5g__firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SNAP-180325/4323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: srv1h_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4324
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4325
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4326
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4327
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4328
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4329
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SRV1-180325/4330

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4331
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4332
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4333
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4334
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4335
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4336
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4337

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: srv1l_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4338
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4339
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4340
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4341
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4342
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4343
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SRV1-180325/4344

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4345
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4346
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4347
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4349
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4350
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4351

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: srv1m_firmware					
Affected Version(s): -					
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur due to improper input validation in clock device. **CVE ID: CVE-2024-53012**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4352
Improper Input Validation	03-Mar-2025	7.8	Memory corruption may occur during communication between primary and guest VM. **CVE ID: CVE-2024-53022**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4353
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4354
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4355
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4356
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur in keyboard virtual device due to guest VM interaction. **CVE ID: CVE-2024-53032**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4357
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53029**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SRV1-180325/4358

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while processing input message passed from FE driver. **CVE ID: CVE-2024-53030**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4359
Improper Input Validation	03-Mar-2025	7.8	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine. **CVE ID: CVE-2024-53031**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4360
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4361
Time-of-check Time-of-use (TOCTOU) Race Condition	03-Mar-2025	7.8	Memory corruption may occur while processing message from frontend during allocation. **CVE ID: CVE-2024-53028**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4362
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4363
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4364
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SRV1-180325/4365

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ssg2115p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4366
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4367
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4368
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4369
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4370
Product: ssg2125p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4371
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	O-QUA-SSG2-180325/4372

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4373
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4374
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SSG2-180325/4375
Product: sw5100p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4376
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4377
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4378

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4379
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4380
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4381
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4382
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4383
Product: sw5100_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4384
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SW51-180325/4385

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4386
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4387
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4389
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4390
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SW51-180325/4391
Product: sxr1120_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SXR1-180325/4392

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4393
Product: sxr1230p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4394
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4395
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4396
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4397
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR1-180325/4398
Product: sxr2130_firmware					
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
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4399
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4400
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4402
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4403
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4404
Product: sxr2230p_firmware					
Affected Version(s): -					
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SXR2-180325/4405

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43060	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4406
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4407
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4408
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4409
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4410
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4411
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-SXR2-180325/4412

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4413
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4414
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4415
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4416
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4417
Product: sxr2250p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4418
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SXR2-180325/4419

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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`s frame processing pipeline. **CVE ID: CVE-2024-49836**	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4420
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4421
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4422
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4423
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4424
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4425
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SXR2-180325/4426

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4427
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4428
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4429
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4430
Product: sxr2330p_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4431
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4432
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-SXR2-180325/4433

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4435
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4436
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-SXR2-180325/4437
Product: talynplus_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-TALY-180325/4438
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-TALY-180325/4439

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-TALY-180325/4440
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-TALY-180325/4441
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-TALY-180325/4442
Product: video_collaboration_vc1_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4443
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4444
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4445
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-VIDE-180325/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4447
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4448
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4449
Product: video_collaboration_vc3_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4450
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4451
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4452
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-VIDE-180325/4453

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4454
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4455
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4456
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4457
Product: video_collaboration_vc5_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4458
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4459
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	O-QUA-VIDE-180325/4460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4461
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4462
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VIDE-180325/4463
Product: vision_intelligence_300__firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VISI-180325/4464
Product: vision_intelligence_400_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VISI-180325/4465
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-VISI-180325/4466

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VISI-180325/4467
Product: vision_intelligence_400__firmware					
Affected Version(s): -					
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-VISI-180325/4468
Product: wcd9306_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4469
Product: wcd9326_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4470
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4471
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4472

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4473
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4474
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4475
Product: wcd9330_firmware					
Affected Version(s): -					
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4476
Product: wcd9335_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4477
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4478

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4479
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4480
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4481
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4482
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4483
Product: wcd9340_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4484
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4485

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4486
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4487
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4489
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4490
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4491
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcd9341_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4493
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4494
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4495
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4496
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4497
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4498
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4499

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4500
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4501
Product: wcd9360_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4502
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4503
Product: wcd9370_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4504
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4505

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4506
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4507
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4508
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4509
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4510
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4511
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4512
Product: wcd9371_firmware					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4513
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4514
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4515
Product: wcd9375_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4516
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4517
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4518
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-180325/4519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-21424	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4520
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4521
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4522
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4523
Product: wcd9378_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4524
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4525
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-WCD9-180325/4526

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4527
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4528
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4529
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4530
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4531
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/security bulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4532
Product: wcd9380_firmware					
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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4533
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4534
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4535
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4536
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4537
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4538
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4539

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4540
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4541
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4542
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4543
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4544
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4545
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4546

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4547
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4548
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4549
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4550
Product: wcd9385_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4551
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4552
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53033	2025-bulletin.html	
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4554
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4555
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4556
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4557
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4558
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4559
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-180325/4560

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43062	bulletin/march-2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4561
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4562
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4563
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4565
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4566
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4567

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4568
Product: wcd9390_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4569
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4570
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4571
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4572
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4573
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCD9-180325/4574

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4575
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4576
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4577
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4578
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4579
Product: wcd9395_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4580
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	O-QUA-WCD9-180325/4581

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4582
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4583
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4584
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4586
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4587
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCD9-180325/4588

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4589
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCD9-180325/4590
Product: wcn3610_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4591
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4592
Product: wcn3615_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4593
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4594

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4595
Product: wcn3620_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4596
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4597
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4598
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4599
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4600
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN3-180325/4601

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4602
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4603
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4604
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4605
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4607
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN3-180325/4608

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4609
Product: wcn3660b_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4610
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4611
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4612
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4613
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4614
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the	https://docs.qualcomm.com/product/publicres	O-QUA-WCN3-180325/4615

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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`s frame processing pipeline. **CVE ID: CVE-2024-49836**	ources/security bulletin/march-2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4616
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4617
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4618
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4619
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4620
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4621
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN3-180325/4622

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')				2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4623
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4624
Product: wcn3680b_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4625
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4626
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4627
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4628
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-180325/4629

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4630
Product: wcn3680_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4631
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4632
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4633
Product: wcn3910_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4634
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4635

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4636
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4637
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4638
Product: wcn3950_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4639
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4640
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4641
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN3-180325/4642

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4643
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4644
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4645
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4646
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4647
Product: wcn3980_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4648
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-180325/4649

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53014	bulletin/march-2025-bulletin.html	
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4650
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4651
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4653
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4654
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4655
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN3-180325/4656

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-38426	2025-bulletin.html	
Product: wcn3988_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4657
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4658
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4659
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4660
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4662
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-180325/4663

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43056	bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4664
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4665
Product: wcn3990_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4666
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4667
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4668
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4669
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a	https://docs.qualcomm.com/product/publicres	O-QUA-WCN3-180325/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			session for any Widevine use case. **CVE ID: CVE-2024-43051**	ources/security bulletin/march-2025-bulletin.html	
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4671
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4672
Product: wcn3999_firmware					
Affected Version(s): -					
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN3-180325/4673
Product: wcn6450_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4674
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4675
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN6-180325/4676

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4677
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4678
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4679
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4680
Product: wcn6650_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4681
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4682
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN6-180325/4683

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4684
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4685
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4686
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4687
Product: wcn6740_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4688
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4689
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports	https://docs.qualcomm.com/product/publicres	O-QUA-WCN6-180325/4690

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and channels in Audio driver. **CVE ID: CVE-2024-53014**	ources/security bulletin/march-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4691
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4692
Product: wcn6755_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4693
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4694
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4696
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	O-QUA-WCN6-180325/4697

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4698
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4699
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN6-180325/4700
Product: wcn7750_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4701
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4702
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4703

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4704
Product: wcn7860_firmware					
Affected Version(s): -					
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4705
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4706
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4707
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4708
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4709
Product: wcn7861_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device.	https://docs.qualcomm.com/product/publicres	O-QUA-WCN7-180325/4710

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-53024	ources/security bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4711
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4712
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4713
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4714
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4715
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4716
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WCN7-180325/4717

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43051	2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4718
Product: wcn7880_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4719
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4720
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4721
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4722
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4723
Product: wcn7881_firmware					
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
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4724
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4725
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4726
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4727
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4728
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4729
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4730
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O	https://docs.qualcomm.com/pr	O-QUA-WCN7-180325/4731

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			operation in a virtual machine. **CVE ID: CVE-2024-43056**	oduct/publicresources/securitybulletin/march-2025-bulletin.html	
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WCN7-180325/4732
Product: wsa8810_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4733
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4734
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4735
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4736
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4737

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4738
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4739
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4740
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4741
Product: wsa8815_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4742
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4743
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4744

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4745
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4746
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4747
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4748
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4749
Product: wsa8830_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4750
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WSA8-180325/4751

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45580	bulletin/march-2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4752
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4753
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4754
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4755
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4756
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4757
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4758

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4759
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4760
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4762
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4763
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4764
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4765

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4766
Product: wsa8832_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4767
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4768
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4769
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4770
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4771
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-43061	2025-bulletin.html	
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP. **CVE ID: CVE-2024-43060**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4773
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4774
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4775
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4776
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4777
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4778
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4779

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4780
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4781
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4782
Product: wsa8835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.8	Memory corruption while processing camera use case IOCTL call. **CVE ID: CVE-2024-43055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4783
Use After Free	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive. **CVE ID: CVE-2024-43061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4784
Use After Free	03-Mar-2025	7.8	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization. **CVE ID: CVE-2024-43062**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4785
Use of Out-of-range Pointer Offset	03-Mar-2025	7.8	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4786

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43060	2025-bulletin.html	
Use After Free	03-Mar-2025	7.8	Memory corruption while processing command in Glink linux. **CVE ID: CVE-2024-43057**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4787
Use After Free	03-Mar-2025	7.8	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node. **CVE ID: CVE-2024-43059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4788
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4789
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4790
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4791
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4792
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4793

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4794
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4795
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4796
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4797
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4798
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4799
Product: wsa8840_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4800

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4801
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4802
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4803
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4804
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4805
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4806
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-	O-QUA-WSA8-180325/4807

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4808
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4809
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4810
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4811
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4812
Product: wsa8845h_firmware					
Affected Version(s): -					
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4813
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WSA8-180325/4814

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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`s frame processing pipeline. **CVE ID: CVE-2024-49836**	bulletin/march-2025-bulletin.html	
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4815
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4816
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4817
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4818
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4819
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4820
Buffer Copy without Checking	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE.	https://docs.qualcomm.com/product/publicres	O-QUA-WSA8-180325/4821

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			**CVE ID: CVE-2024-53027**	ources/security bulletin/march-2025-bulletin.html	
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4822
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4823
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4824
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4825
Product: wsa8845_firmware					
Affected Version(s): -					
NULL Pointer Dereference	03-Mar-2025	7.8	Memory corruption in display driver while detaching a device. **CVE ID: CVE-2024-53024**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4826
Use After Free	03-Mar-2025	7.8	Memory corruption may occur while accessing a variable during extended back to back tests. **CVE ID: CVE-2024-53023**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4827

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur while validating ports and channels in Audio driver. **CVE ID: CVE-2024-53014**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4828
Use After Free	03-Mar-2025	7.8	Memory corruption while calling the NPU driver APIs concurrently. **CVE ID: CVE-2025-21424**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4829
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address. **CVE ID: CVE-2024-53033**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4830
Untrusted Pointer Dereference	03-Mar-2025	7.8	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset. **CVE ID: CVE-2024-53034**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4831
Use After Free	03-Mar-2025	7.8	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation. **CVE ID: CVE-2024-45580**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4832
Improper Validation of Array Index	03-Mar-2025	7.8	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline. **CVE ID: CVE-2024-49836**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	7.5	Transient DOS may occur while processing the country IE. **CVE ID: CVE-2024-53027**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4834

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	03-Mar-2025	5.5	Transient DOS can occur while processing UCI command. **CVE ID: CVE-2024-53025**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4835
Improper Authorization	03-Mar-2025	5.5	Information disclosure while deriving keys for a session for any Widevine use case. **CVE ID: CVE-2024-43051**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4836
Buffer Over-read	03-Mar-2025	5.5	Transient DOS during hypervisor virtual I/O operation in a virtual machine. **CVE ID: CVE-2024-43056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4837
Improper Authentication	03-Mar-2025	5.4	While processing the authentication message in UE, improper authentication may lead to information disclosure. **CVE ID: CVE-2024-38426**	https://docs.qualcomm.com/product/publicresources/securitybulletin/march-2025-bulletin.html	O-QUA-WSA8-180325/4838
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 7.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	6.7	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based out-of-bounds writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass.	N/A	O-RED-ENTE-180325/4839

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45782		
Out-of-bounds Write	03-Mar-2025	6.4	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections. **CVE ID: CVE-2025-0678**	N/A	O-RED-ENTE-180325/4840
Integer Overflow or Wraparound	03-Mar-2025	4.1	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash. **CVE ID: CVE-2024-45778**	N/A	O-RED-ENTE-180325/4841
Affected Version(s): 8.0					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	03-Mar-2025	6.7	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based	N/A	O-RED-ENTE-180325/4842

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass. **CVE ID: CVE-2024-45782**		
Out-of-bounds Write	03-Mar-2025	6.4	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections. **CVE ID: CVE-2025-0678**	N/A	O-RED-ENTE-180325/4843
Integer Overflow or Wraparound	03-Mar-2025	4.1	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash. **CVE ID: CVE-2024-45778**	N/A	O-RED-ENTE-180325/4844
Affected Version(s): 9.0					
Buffer Copy without Checking Size of Input ('Classic	03-Mar-2025	6.7	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a	N/A	O-RED-ENTE-180325/4845

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based out-of-bounds writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass. **CVE ID: CVE-2024-45782**		
Out-of-bounds Write	03-Mar-2025	6.4	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections. **CVE ID: CVE-2025-0678**	N/A	O-RED-ENTE-180325/4846
Integer Overflow or Wraparound	03-Mar-2025	4.1	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash. **CVE ID: CVE-2024-45778**	N/A	O-RED-ENTE-180325/4847

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: Tenda					
Product: ac6_firmware					
Affected Version(s): 15.03.05.16					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Mar-2025	8.8	A vulnerability, which was classified as critical, has been found in Tenda AC6 15.03.05.16. Affected by this issue is some unknown functionality of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1814**	N/A	O-TEN-AC6_-180325/4848
Product: ac8_firmware					
Affected Version(s): 16.03.34.06					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Mar-2025	8.8	A vulnerability was found in Tenda AC8 16.03.34.06 and classified as critical. This issue affects the function sub_49E098 of the file /goform/SetIpMacBind of the component Parameter Handler. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1853**	N/A	O-TEN-AC8_-180325/4849
Product: tx3_firmware					
Affected Version(s): 16.03.13.11					
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability, which was classified as critical, has been found in Tenda TX3 16.03.13.11_multi. This issue affects some unknown processing of the file /goform/SetNetControlList. The manipulation of the	N/A	O-TEN-TX3_-180325/4850

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument list leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1897**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability classified as critical was found in Tenda TX3 16.03.13.11_multi. This vulnerability affects unknown code of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1896**	N/A	O-TEN-TX3_-180325/4851
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability classified as critical has been found in Tenda TX3 16.03.13.11_multi. This affects an unknown part of the file /goform/setMacFilterCfg. The manipulation of the argument deviceList leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1895**	N/A	O-TEN-TX3_-180325/4852
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability, which was classified as critical, was found in Tenda TX3 16.03.13.11_multi. Affected is an unknown function of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime/schedEndTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit	N/A	O-TEN-TX3_-180325/4853

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. **CVE ID: CVE-2025-1898**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-Mar-2025	6.5	A vulnerability has been found in Tenda TX3 16.03.13.11_multi and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setPptpUserList. The manipulation of the argument list leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-1899**	N/A	O-TEN-TX3_-180325/4854
Vendor: Vmware					
Product: esxi					
Affected Version(s): 7.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4855
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4856

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process. **CVE ID: CVE-2025-22226**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4857
Affected Version(s): 8.0					
Time-of-check Time-of-use (TOCTOU) Race Condition	04-Mar-2025	9.3	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE ID: CVE-2025-22224**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4858
Out-of-bounds Write	04-Mar-2025	8.2	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox. **CVE ID: CVE-2025-22225**	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4859
Out-of-bounds Read	04-Mar-2025	7.1	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process.	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390	O-VMW-ESXI-180325/4860

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-22226		

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

* stands for all versions