https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Jan 2025 Vol. 12 No. 01

Table of Content

Vendor	Product	Page Number
Qualcomm	fastconnect_6200	18
	fastconnect_6700	19
	fastconnect_6800	20
	fastconnect_6900	20
	fastconnect_7800	22
	flight_rb5_5g	24
	immersive_home_214	24
	immersive_home_216	25
	immersive_home_316	25
	immersive_home_318	25
	immersive_home_3210	25
	immersive_home_326	26
	ipq5010	26
	ipq5028	26
	ipq5300	26
	ipq5302	26
	ipq5312	27
	ipq5332	27
	ipq6000	27
	ipq6010	27
	ipq6018	28
	ipq6028	28
	ipq8070a	28
	ipq8071a	28
	ipq8072a	28
	ipq8074a	29
	ipq8076	29
	ipq8076a	29
	ipq8078	29
	ipq8078a	30
	ipq8173	30
	ipq8174	30
	ipq9008	30

Vendor	Product	Page Number
Qualcomm	snapdragon_x35_5g_modem-rf	124
	snapdragon_x55_5g_modem-rf	124
	snapdragon_x65_5g_modem-rf	124
	snapdragon_x72_5g_modem-rf	125
	snapdragon_x75_5g_modem-rf	125
	snapdragon_xr2_5g	126
	srv1h	126
	srv1l	127
	srv1m	128
	ssg2115p	129
	ssg2125p	130
	sw5100	130
	sw5100p	131
	sxr1230p	131
	sxr2130	132
	sxr2230p	132
	sxr2250p	133
	sxr2330p	133
	talynplus	133
	video_collaboration_vc1	134
	video_collaboration_vc3	134
	video_collaboration_vc5	135
	wcd9335	135
	wcd9340	136
	wcd9341	136
	wcd9370	137
	wcd9375	138
	wcd9378	139
	wcd9380	139
	wcd9385	141
	wcd9390	143
	wcd9395	144
	wcn3620	145

Vendor	Product	Page Number
Qualcomm	wcd9341_firmware	456
	wcd9370_firmware	456
	wcd9375_firmware	457
	wcd9378_firmware	458
	wcd9380_firmware	458
	wcd9385_firmware	460
	wcd9390_firmware	462
	wcd9395_firmware	463
	wcn3620_firmware	464
	wcn3660b_firmware	464
	wcn3680b_firmware	465
	wcn3950_firmware	465
	wcn3980_firmware	466
	wcn3988_firmware	466
	wcn3990_firmware	467
	wcn6450_firmware	467
	wcn6650_firmware	468
	wcn6740_firmware	468
	wcn6755_firmware	468
	wcn7860_firmware	469
	wcn7861_firmware	469
	wcn7880_firmware	469
	wcn7881_firmware	470
	wsa8810_firmware	470
	wsa8815_firmware	471
	wsa8830_firmware	472
	wsa8832_firmware	473
	wsa8835_firmware	474
	wsa8840_firmware	475
	wsa8845h_firmware	477
	wsa8845_firmware	479

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: Apache					
Product: openmeetings					
Affected Version(s): From (including) 2.1 Up to (excluding) 8.0.0					
Deserialization of Untrusted Data	08-Jan-2025	9.8	Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.1.0 before 8.0.0 Description: Default clustering instructions at https://openmeetings.apache.org/Clustering.html doesn't specify white/black lists for OpenJPA this leads to possible deserialisation of untrusted data. Users are recommended to upgrade to version 8.0.0 and update their startup scripts to include the relevant 'openjpa.serialization.class.blacklist' and 'openjpa.serialization.class.whitelist' configurations as shown in the documentation. **CVE ID: CVE-2024-54676**	https://lists.apache.org/thread/o0k05jxrt5tp4nm45lj14yfjxmg67m95	A-APA-OPEN-200125/1
Vendor: campcodes					
Product: project_management_system					
Affected Version(s): 1.0					
Improper Access Control	04-Jan-2025	6.3	A vulnerability was found in Campcodes Project Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /forms/update_forms.php?action=change_pic2&id=4. The manipulation of the	N/A	A-CAM-PROJ-200125/2

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 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-2025-0213**		
Product: school_faculty_scheduling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jan-2025	7.3	A vulnerability has been found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-0210**	N/A	A-CAM-SCHO-200125/3
External Control of File Name or Path	04-Jan-2025	6.3	A vulnerability was found in Campcodes School Faculty Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-0211**	N/A	A-CAM-SCHO-200125/4
Product: student_grading_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	04-Jan-2025	6.3	A vulnerability was found in Campcodes Student Grading System 1.0. It has been	N/A	A-CAM-STUD-200125/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			classified as critical. This affects an unknown part of the file /view_students.php. The manipulation of the argument id 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-2025-0212**		
Vendor: code-projects					
Product: local_storage_todo_app					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability has been found in code-projects Local Storage Todo App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /js-todo-app/index.html. The manipulation of the argument Add 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-2025-0228**	N/A	A-COD-LOCA-200125/6
Product: online_shoe_store					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jan-2025	7.3	A vulnerability, which was classified as critical, has been found in code-projects Online Shoe Store 1.0. Affected by this issue is some unknown functionality of the file /function/login.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-COD-ONLI-200125/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2025-0207		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-Jan-2025	6.3	A vulnerability, which was classified as critical, was found in code-projects Online Shoe Store 1.0. This affects an unknown part of the file /summary.php. The manipulation of the argument tid 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-2025-0208**	N/A	A-COD-ONLI-200125/8
Vendor: codezips					
Product: blood_bank_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability was found in Codezips Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /successadmin.php. The manipulation of the argument psw 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-2025-0232**	N/A	A-COD-BLOO-200125/9
Product: gym_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability has been found in Codezips Gym Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard/admin/submit_payments.php. The	N/A	A-COD-GYM_-200125/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument m_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-0231**		
Product: project_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	7.3	A vulnerability was found in Codezips Project Management System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/forms/course.php. The manipulation of the argument course_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-0233**	N/A	A-COD-PROJ-200125/11
Vendor: Dell					
Product: powerscale_onefs					
Affected Version(s): From (including) 8.2.2 Up to (excluding) 9.4.0.20					
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-47475**	https://www.dell.com/support/kbdoc/en-us/000242681/dsa-2024-417-security-update-for-dell-powerscale-onefs-for-security-vulnerability	A-DEL-POWE-200125/12
Affected Version(s): From (including) 9.5.0.0 Up to (including) 9.5.0.8					
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource	https://www.dell.com/support/kbdoc/en-us/000242681/dsa-2024-417-	A-DEL-POWE-200125/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-47475**	security-update-for-dell-powerscale-onefs-for-security-vulnerability	
Affected Version(s): From (including) 9.6.0 Up to (including) 9.7.0.3					
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-47475**	https://www.dell.com/support/kbdoc/en-us/000242681/dsa-2024-417-security-update-for-dell-powerscale-onefs-for-security-vulnerability	A-DEL-POWE-200125/14
Affected Version(s): From (including) 9.8.0.0 Up to (including) 9.8.0.2					
Incorrect Permission Assignment for Critical Resource	06-Jan-2025	5	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service. **CVE ID: CVE-2024-47475**	https://www.dell.com/support/kbdoc/en-us/000242681/dsa-2024-417-security-update-for-dell-powerscale-onefs-for-security-vulnerability	A-DEL-POWE-200125/15
Vendor: emlog					
Product: emlog					
Affected Version(s): From (including) 2.4.0 Up to (including) 2.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic has been found in Emlog Pro up to 2.4.3. Affected is an unknown function of the file /admin/article.php?action=upload_cover of the component Cover Upload Handler. The manipulation of the argument image leads to cross site scripting. It is possible to launch the	N/A	A-EML-EMLO-200125/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-13140**		
Vendor: fabianros					
Product: responsive_hotel_site					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability, which was classified as critical, was found in code-projects Responsive Hotel Site 1.0. Affected is an unknown function of the file /admin/print.php. The manipulation of the argument pid 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-2025-0230**	N/A	A-FAB-RESP-200125/17
Product: travel_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Jan-2025	6.3	A vulnerability, which was classified as critical, has been found in code-projects Travel Management System 1.0. This issue affects some unknown processing of the file /enquiry.php. The manipulation of the argument pid/t1/t2/t3/t4/t5/t6/t7 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2025-0229**	N/A	A-FAB-TRAV-200125/18
Vendor: Fortinet					
Product: fortiproxy					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.20					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authentication Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. **CVE ID: CVE-2024-55591**	https://fortiguard.fortinet.com/psirt/FG-IR-24-535	A-FOR-FORT-200125/19
Affected Version(s): From (including) 7.2.0 Up to (excluding) 7.2.13					
Authentication Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. **CVE ID: CVE-2024-55591**	https://fortiguard.fortinet.com/psirt/FG-IR-24-535	A-FOR-FORT-200125/20
Vendor: ivanti					
Product: connect_secure					
Affected Version(s): * Up to (excluding) 9.1					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/21
Affected Version(s): 21.12					

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
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/22
Affected Version(s): 21.9					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/23
Affected Version(s): 22.1					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/24
Affected Version(s): 22.7					
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-	A-IVA-CONN-200125/25

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
			before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2025-0282**	CVE-2025-0282-CVE-2025-0283	
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/26
Affected Version(s): 9.1					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/27
Affected Version(s): From (including) 22.2 Up to (excluding) 22.7					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-CONN-200125/28
Product: neurons_for_zero-trust_access					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/29
Affected Version(s): 22.2					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/30
Affected Version(s): 22.3					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/31
Affected Version(s): 22.4					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-	A-IVA-NEUR-200125/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	
Affected Version(s): 22.5					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/33
Affected Version(s): 22.6					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/34
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2025-0282**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-NEUR-200125/35
Stack-based	08-Jan-2025	7	A stack-based buffer	https://forums.i	A-IVA-NEUR-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	vanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	200125/36
Product: policy_secure					
Affected Version(s): * Up to (excluding) 22.7					
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges. **CVE ID: CVE-2025-0283**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-POLI-200125/37
Stack-based Buffer Overflow	08-Jan-2025	9	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution. **CVE ID: CVE-2025-0282**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-POLI-200125/38
Stack-based Buffer Overflow	08-Jan-2025	7	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	A-IVA-POLI-200125/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to escalate their privileges. **CVE ID: CVE-2025-0283**		
Vendor: osuuu					
Product: lightpicture					
Affected Version(s): 1.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload Handler. The manipulation of the argument file 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-2024-13141**	N/A	A-OSU-LIGH-200125/40
Affected Version(s): 1.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload Handler. The manipulation of the argument file 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-2024-13141**	N/A	A-OSU-LIGH-200125/41
Affected Version(s): 1.2.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site	05-Jan-2025	3.5	A vulnerability classified as problematic was found in osuuu LightPicture up to 1.2.2. This vulnerability affects unknown code of the file /api/upload of the component SVG File Upload	N/A	A-OSU-LIGH-200125/42

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Handler. The manipulation of the argument file 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-2024-13141**		
Vendor: wangl1989					
Product: mysiteforme					
Affected Version(s): 1.0					
Server-Side Request Forgery (SSRF)	05-Jan-2025	6.3	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been rated as critical. This issue affects the function doContent of the file src/main/java/com/mysiteform/admin/controller/system/FileController. The manipulation of the argument content leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-13139**	N/A	A-WAN-MYSI-200125/43
Improper Input Validation	05-Jan-2025	6.3	A vulnerability was found in wangl1989 mysiteforme 1.0 and classified as critical. Affected by this issue is the function rememberMeManager of the file src/main/java/com/mysiteforme/admin/config/ShiroConfig.java. The manipulation leads to deserialization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID: CVE-2024-13136**	N/A	A-WAN-MYSI-200125/44
Improper	05-Jan-2025	4.7	A vulnerability was found in	N/A	A-WAN-MYSI-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Access Control			wangl1989 mysiteforme 1.0. It has been declared as critical. This vulnerability affects the function upload of the file src/main/java/com/mysiteform/admin/service/ipl/LocalUploadServiceImpl. The manipulation of the argument test 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-2024-13138**		200125/45
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability was found in wangl1989 mysiteforme 1.0. It has been classified as problematic. This affects the function RestResponse of the file src/main/java/com/mysiteforme/admin/controller/system/SiteController. The manipulation 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. **CVE ID: CVE-2024-13137**	N/A	A-WAN-MYSI-200125/46
Vendor: zerowdd					
Product: studentmanager					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Jan-2025	2.4	A vulnerability was found in ZeroWdd studentmanager 1.0. It has been declared as problematic. This vulnerability affects the function submitAddRole of the file src/main/java/com/zero/system/controller/RoleController. java. The manipulation of the argument name leads to cross site scripting. The	N/A	A-ZER-STUD-200125/47

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be initiated remotely. **CVE ID: CVE-2024-13142**		
Hardware					
Vendor: Qualcomm					
Product: aqt1000					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-AQT1-200125/48
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-AQT1-200125/49
Product: ar8035					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-AR80-200125/50
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-AR80-200125/51
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qualcomm.com/product/publicresources/security	H-QUA-AR80-200125/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	bulletin/january-2025-bulletin.html	
Product: c-v2x_9150					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-C-V2-200125/53
Product: csr8811					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-CSR8-200125/54
Product: csrb31024					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-CSRB-200125/55
Product: fastconnect_6200					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/56
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	H-QUA-FAST-200125/57

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january -2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/58
Product: fastconnect_6700					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/59
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/60
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/61
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/62
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-FAST-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/63
Product: fastconnect_6800					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/64
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/65
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/66
Product: fastconnect_6900					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/67
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/68
Stack-based	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	H-QUA-FAST-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/69
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/70
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/71
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/72
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/73
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/74
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-FAST-200125/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/76
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/77
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/78
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/79
Product: fastconnect_7800					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/80
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/81
Buffer Copy without Checking	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to	https://docs.qualcomm.com/product/publicres	H-QUA-FAST-200125/82

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/83
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/84
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/85
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/86
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/87
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-FAST-200125/88

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/89
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/90
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/91
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FAST-200125/92
Product: flight_rb5_5g					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-FLIG-200125/93
Product: immersive_home_214					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-IMME-200125/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: immersive_home_216					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IMME-200125/95
Product: immersive_home_316					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IMME-200125/96
Product: immersive_home_318					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IMME-200125/97
Product: immersive_home_3210					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IMME-200125/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: immersive_home_326					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IMME-200125/99
Product: ipq5010					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ5-200125/100
Product: ipq5028					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ5-200125/101
Product: ipq5300					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ5-200125/102
Product: ipq5302					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ5-200125/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: ipq5312					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ5-200125/104
Product: ipq5332					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ5-200125/105
Product: ipq6000					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ6-200125/106
Product: ipq6010					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ6-200125/107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq6018					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ6-200125/108
Product: ipq6028					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ6-200125/109
Product: ipq8070a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/110
Product: ipq8071a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/111
Product: ipq8072a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ8-200125/112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: ipq8074a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/113
Product: ipq8076					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/114
Product: ipq8076a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/115
Product: ipq8078					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipq8078a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/117
Product: ipq8173					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/118
Product: ipq8174					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ8-200125/119
Product: ipq9008					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ9-200125/120
Product: ipq9048					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-IPQ9-200125/121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: ipq9554					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ9-200125/122
Product: ipq9570					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ9-200125/123
Product: ipq9574					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-IPQ9-200125/124
Product: msm8996au					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-MSM8-200125/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image. **CVE ID: CVE-2024-45555**		
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-MSM8-200125/126
Product: qam8255p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/127
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/128
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/129
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-QAM8-200125/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/131
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/132
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/133
Product: qam8295p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/134
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/135
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver,	https://docs.qualcomm.com/pr	H-QUA-QAM8-200125/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/137
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/138
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/139
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/140
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/141
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/142
Buffer Over-	06-Jan-2025	5.5	Transient DOS can occur	https://docs.qu	H-QUA-QAM8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/143
Product: qam8620p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/144
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/145
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/146
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/147
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-	https://docs.qualcomm.com/product/publicres	H-QUA-QAM8-200125/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FastRPC backend. **CVE ID: CVE-2024-45559**	ources/security bulletin/january -2025-bulletin.html	
Product: qam8650p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/149
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/150
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/151
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/152
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QAM8-200125/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-23366	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/154
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/155
Product: qam8775p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/156
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/157
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/158
N/A	06-Jan-2025	7.5	Uncontrolled resource	https://docs.qu	H-QUA-QAM8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/159
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/160
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/161
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAM8-200125/162
Product: qamsrv1h					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/163
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/165
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/166
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/167
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/168
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/169
Product: qamsrv1m					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tampered IFS2 system image. **CVE ID: CVE-2024-45555**		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/171
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/172
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/173
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QAMS-200125/174
Product: qca0000					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA0-200125/175
Product: qca1062					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA1-200125/176
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA1-200125/177
Product: qca1064					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA1-200125/178
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA1-200125/179
Product: qca2062					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/180
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/181
Product: qca2064					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/182
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/183
Product: qca2065					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/184
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/185
Product: qca2066					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA2-200125/187
Product: qca4024					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA4-200125/188
Product: qca6174a					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/189
Product: qca6310					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/190
Product: qca6320					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/191
Product: qca6391					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	H-QUA-QCA6-200125/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/193
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/194
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/195
Product: qca6420					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/196
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/197
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
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/198
Product: qca6430					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/199
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/200
Product: qca6436					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/201
Product: qca6554a					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/202
Product: qca6564a					
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
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/203
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/204
Product: qca6564au					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/205
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/206
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/207

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qca6574					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/208
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/209
Product: qca6574a					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/210
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/211
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-QCA6-200125/212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/213
Product: qca6574au					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/214
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/215
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/216
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCA6-200125/217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. **CVE ID: CVE-2024-43064**	bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/218
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/219
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/220
Product: qca6584au					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/221
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/223
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/224
Product: qca6595					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/225
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/226
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/227

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45558		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/228
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/229
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/230
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/231
Product: qca6595au					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/232
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QCA6-200125/233

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/234
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/235
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/236
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/237
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/238
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/239

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/240
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/241
Product: qca6678aq					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/242
Product: qca6688aq					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/243
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/244

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/245
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/246
Product: qca6696					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/247
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/248
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/249
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCA6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/250
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/251
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/252
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/253
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/254
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/255
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/256

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6698aq					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/257
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/258
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/259
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/260
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/261
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qualcomm.com/pr	H-QUA-QCA6-200125/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/263
Product: qca6777aq					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/264
Product: qca6787aq					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/265
Product: qca6797aq					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA6-200125/266
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCA6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/267
Product: qca8075					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/268
Product: qca8081					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/269
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/270
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/271
Product: qca8082					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/272
Product: qca8084					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/273
Product: qca8085					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/274
Product: qca8337					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/275
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QCA8-200125/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/277
Product: qca8386					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA8-200125/278
Product: qca9367					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA9-200125/279
Product: qca9377					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA9-200125/280
Product: qca9888					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-QCA9-200125/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: qca9889					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCA9-200125/282
Product: qcc2073					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/283
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/285
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/286
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board	https://docs.qualcomm.com/product/publicres	H-QUA-QCC2-200125/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			data to WLAN driver. **CVE ID: CVE-2024-45542**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/288
Product: qcc2076					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/289
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/291
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/292
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/293

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC2-200125/294
Product: qcc710					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC7-200125/295
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC7-200125/296
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCC7-200125/297
Product: qcf8000					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCF8-200125/298
Product: qcf8000sfp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCF8-200125/299
Product: qcf8001					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCF8-200125/300
Product: qcm4325					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM4-200125/301
Product: qcm4490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM4-200125/302
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-QCM4-200125/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Product: qcm5430					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM5-200125/304
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM5-200125/305
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM5-200125/306
Product: qcm6490					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM6-200125/307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM6-200125/308
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCM6-200125/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID without checking the IE length. **CVE ID: CVE-2024-45558**	bulletin/january-2025-bulletin.html	
Product: qcm8550					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM8-200125/310
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM8-200125/311
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM8-200125/312
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCM8-200125/313
Product: qcn5022					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/314
Product: qcn5024					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/315
Product: qcn5052					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/316
Product: qcn5122					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/317
Product: qcn5124					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/318
Product: qcn5152					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-QCN5-200125/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcn5154					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/320
Product: qcn5164					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN5-200125/321
Product: qcn6023					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/322
Product: qcn6024					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/323
Product: qcn6112					
Affected Version(s): -					
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-QCN6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/324
Product: qcn6122					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/325
Product: qcn6132					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/326
Product: qcn6224					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/327
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/328

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45558		
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/329
Product: qcn6274					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/330
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/331
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/332
Product: qcn6402					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: qcn6412					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/334
Product: qcn6422					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/335
Product: qcn6432					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN6-200125/336
Product: qcn7605					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN7-200125/337
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QCN7-200125/338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025-bulletin.html	
Product: qcn7606					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN7-200125/339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN7-200125/340
Product: qcn9000					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/341
Product: qcn9012					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/342
Product: qcn9022					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-QCN9-200125/343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcn9024					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/344
Product: qcn9070					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/345
Product: qcn9072					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/346
Product: qcn9074					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/347
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qualcomm.com/product/publicresources/security	H-QUA-QCN9-200125/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	bulletin/january-2025-bulletin.html	
Product: qcn9100					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/349
Product: qcn9160					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/350
Product: qcn9274					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCN9-200125/351
Product: qcs410					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS4-200125/352
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qualcomm.com/pr	H-QUA-QCS4-200125/353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	oduct/publicresources/security bulletin/january-2025-bulletin.html	
Product: qcs4490					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-QCS4-200125/354
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-QCS4-200125/355
Product: qcs5430					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-QCS5-200125/356
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-QCS5-200125/357
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-QCS5-200125/358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: qcs610					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/359
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/360
Product: qcs6490					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/361
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/362
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/363
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QCS6-200125/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS6-200125/365
Product: qcs7230					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS7-200125/366
Product: qcs8250					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/367
Product: qcs8550					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/369
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/370
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/371
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/372
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS8-200125/373
Product: qcs9100					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QCS9-200125/374

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qdu1000					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QDU1-200125/375
Product: qdu1010					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QDU1-200125/376
Product: qdu1110					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QDU1-200125/377
Product: qdu1210					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-QDU1-200125/378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	-2025-bulletin.html	
Product: qdx1010					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QDX1-200125/379
Product: qdx1011					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QDX1-200125/380
Product: qep8111					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QEP8-200125/381
Product: qfw7114					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/382
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/383
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/384
Product: qfw7124					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/385
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QFW7-200125/387
Product: qrb5165n					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QRB5-200125/388
Product: qru1032					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QRU1-200125/389
Product: qru1052					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QRU1-200125/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qru1062					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QRU1-200125/391
Product: qsm8250					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QSM8-200125/392
Product: qxm8083					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-QXM8-200125/393
Product: robotics_rb5					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-ROBO-200125/394

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sa6145p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/395
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/396
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/397
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/398
Product: sa6150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/400
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/401
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/402
Product: sa6155					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/403
Product: sa6155p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image. **CVE ID: CVE-2024-45555**		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/405
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/406
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/407
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/408
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA61-200125/409
Product: sa7255p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA72-200125/410

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA72-200125/411
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA72-200125/412
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA72-200125/413
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA72-200125/414
Product: sa7775p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-SA77-200125/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA77-200125/416
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA77-200125/417
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA77-200125/418
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA77-200125/419
Product: sa8145p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tampered IFS2 system image. **CVE ID: CVE-2024-45555**		
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/421
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/422
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/423
Product: sa8150p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/424
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/425
Use of Out-of-range Pointer	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is	https://docs.qualcomm.com/product/publicres	H-QUA-SA81-200125/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Offset			missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/427
Product: sa8155					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/428
Product: sa8155p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/429
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/430

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/431
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/432
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/433
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/434
Product: sa8195p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/435
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA81-200125/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/437
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/438
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/439
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA81-200125/440
Product: sa8255p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/442
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/443
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/444
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/445
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/446
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/447

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
Product: sa8295p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/448
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/449
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/450
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/451
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/452
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to	https://docs.qualcomm.com/pr	H-QUA-SA82-200125/453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap the DMA buffers. **CVE ID: CVE-2024-33055**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/454
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/455
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/456
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA82-200125/457
Product: sa8530p					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/458
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-SA85-200125/459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sa8540p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/460
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/461
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/462
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/463
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/464
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API.	https://docs.qualcomm.com/product/publicres	H-QUA-SA85-200125/465

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43063	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA85-200125/466
Product: sa8620p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/467
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/468
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/469
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-SA86-200125/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/471
Product: sa8650p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/472
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/473
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/474
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/475

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
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/476
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/477
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA86-200125/478
Product: sa8770p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/479
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/480
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SA87-200125/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. **CVE ID: CVE-2024-43064**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/482
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/483
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/484
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/485
Product: sa8775p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/486
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	H-QUA-SA87-200125/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/488
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/489
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/490
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/491
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA87-200125/492
Product: sa9000p					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qualcomm.com/product/publicres	H-QUA-SA90-200125/493

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
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	ources/security bulletin/january -2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/494
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/495
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/496
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/497
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/498

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/499
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SA90-200125/500
Product: sc8180x-aaab					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/501
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/502
Product: sc8180x-acaf					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/503
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/504
Product: sc8180x-ad					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/505
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/506
Product: sc8180xp-aaab					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/508
Product: sc8180xp-acaf					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/509
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/510
Product: sc8180xp-ad					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/511
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/512
Product: sc8180x\+sdx55					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/513
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC81-200125/514
Product: sc8280xp-abbb					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC82-200125/515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC82-200125/516
Product: sc8380xp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/517
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/518
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/520
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/521
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SC83-200125/522
Product: sd835					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-SD83-200125/523

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sound model driver. **CVE ID: CVE-2024-33067**	-2025-bulletin.html	
Product: sd865_5g					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SD86-200125/524
Product: sdm429w					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SDM4-200125/525
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SDM4-200125/526
Product: sdx55					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SDX5-200125/527
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-SDX5-200125/528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: sdx65m					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SDX6-200125/529
Product: sd_8_gen1_5g					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SD_8-200125/530
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SD_8-200125/531
Product: sg4150p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SG41-200125/532
Product: sg8275p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SG82-200125/533
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SG82-200125/534
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SG82-200125/535
Product: sm4635					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM46-200125/536
Product: sm6250					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM62-200125/537
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM62-200125/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-45541**	bulletin/january-2025-bulletin.html	
Product: sm6650					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM66-200125/539
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM66-200125/540
Product: sm7635					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/541
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/542
Product: sm7675					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/543
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/544
Product: sm7675p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/545
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM76-200125/546
Product: sm8550p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM85-200125/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM85-200125/548
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM85-200125/549
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM85-200125/550
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM85-200125/551
Product: sm8635					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM86-200125/552
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qualcomm.com/product/publicresources/security	H-QUA-SM86-200125/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID without checking the IE length. **CVE ID: CVE-2024-45558**	bulletin/january-2025-bulletin.html	
Product: sm8635p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM86-200125/554
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM86-200125/555
Product: sm8750					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM87-200125/556
Product: sm8750p					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SM87-200125/557
Product: snapdragon_429_mobile					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/558
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/559
Product: snapdragon_460_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/560
Product: snapdragon_480\+_5g_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/561
Product: snapdragon_480_5g_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	H-QUA-SNAP-200125/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: snapdragon_4_gen_1_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/563
Product: snapdragon_4_gen_2_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/564
Product: snapdragon_662_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/565

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Product: snapdragon_680_4g_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/566
Product: snapdragon_685_4g_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/567
Product: snapdragon_695_5g_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/568
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Buffer Copy without Checking	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-200125/569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			data. **CVE ID: CVE-2024-45541**	ources/security bulletin/january -2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-SNAP-200125/570
Product: snapdragon_7c_compute_platform					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-SNAP-200125/571
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-SNAP-200125/572
Product: snapdragon_7c_gen_2_compute_platform					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-SNAP-200125/573
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-SNAP-200125/574
Product: snapdragon_820_automotive					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-200125/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/576
Product: snapdragon_835_mobile_pc					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/577
Product: snapdragon_865\+_5g_mobile					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/578
Product: snapdragon_865_5g_mobile					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_870_5g_mobile					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/580
Product: snapdragon_8\+_gen_1_mobile					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/581
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/582
Product: snapdragon_8\+_gen_2_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/583
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-SNAP-200125/584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/585
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/586
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/587
Product: snapdragon_8_gen_1_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/588
Product: snapdragon_8_gen_2_mobile					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/589

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/590
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/591
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/592
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/593
Product: snapdragon_8_gen_3_mobile					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/594
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/596
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/597
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/598
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/599
Product: snapdragon_ar1_gen_1					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/600
Product: snapdragon_ar2_gen_1					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-200125/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january -2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/602
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/603
Product: snapdragon_auto_5g_modem-rf_gen_2					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/604
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/605
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-200125/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	ources/security bulletin/january -2025-bulletin.html	
Product: snapdragon_w5\+_gen_1_wearable					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/607
Product: snapdragon_x35_5g_modem-rf					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/608
Product: snapdragon_x55_5g_modem-rf					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/609
Product: snapdragon_x65_5g_modem-rf					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-SNAP-200125/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: snapdragon_x72_5g_modem-rf					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/611
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/612
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/613
Product: snapdragon_x75_5g_modem-rf					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/614
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	H-QUA-SNAP-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/615
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/616
Product: snapdragon_xr2_5g					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SNAP-200125/617
Product: srv1h					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/618
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/619

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/620
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/621
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/622
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/623
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/624
Product: srv1l					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			image. **CVE ID: CVE-2024-45555**		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/626
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/627
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/628
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/629
Product: srv1m					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/630

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/631
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/632
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/633
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SRV1-200125/634
Product: ssg2115p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SSG2-200125/635
Use of Out-	06-Jan-2025	6.7	Memory corruption when	https://docs.qu	H-QUA-SSG2-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of-range Pointer Offset			input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/636
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SSG2-200125/637
Product: ssg2125p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SSG2-200125/638
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SSG2-200125/639
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SSG2-200125/640
Product: sw5100					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SW51-200125/641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SW51-200125/642
Product: sw5100p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SW51-200125/643
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SW51-200125/644
Product: sxr1230p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR1-200125/645
Use of Out-of-range	06-Jan-2025	6.7	Memory corruption when input parameter validation	https://docs.qualcomm.com/pr	H-QUA-SXR1-200125/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset			for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR1-200125/647
Product: sxr2130					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/648
Product: sxr2230p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/649
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/650
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-SXR2-200125/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sxr2250p					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/652
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/653
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/654
Product: sxr2330p					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-SXR2-200125/655
Product: talynplus					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-TALY-200125/656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-TALY-200125/657
Product: video_collaboration_vc1					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-VIDE-200125/658
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-VIDE-200125/659
Product: video_collaboration_vc3					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-VIDE-200125/660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-VIDE-200125/661
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	H-QUA-VIDE-200125/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-VIDE-200125/663
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-VIDE-200125/664
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-VIDE-200125/665
Product: video_collaboration_vc5					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-VIDE-200125/666
Product: wcd9335					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qualcomm.com/product/publicresources/security bulletin/january -2025-bulletin.html	H-QUA-WCD9-200125/667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067		
Product: wcd9340					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/668
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/669
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/670
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/671
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/672
Product: wcd9341					
Affected Version(s): -					
Stack-based Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qualcomm.com/pr	H-QUA-WCD9-200125/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	oduct/publicresources/security bulletin/january-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/674
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/675
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/676
Product: wcd9370					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/677
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/678
Buffer Copy without	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qualcomm.com/pr	H-QUA-WCD9-200125/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			user-space to read board data. **CVE ID: CVE-2024-45541**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/680
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/681
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/682
Product: wcd9375					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/683
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/684
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-WCD9-200125/685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/686
Product: wcd9378					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/687
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/688
Product: wcd9380					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/689
Buffer Copy	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	H-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/690
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/691
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/693
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/694
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/695
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/696
Use After	06-Jan-2025	6.7	Memory corruption while	https://docs.qu	H-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/697
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/698
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/699
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/700
Product: wcd9385					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/701
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/702
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-WCD9-200125/703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45550	-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/704
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/705
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/706
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/707
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/708
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/709
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command	https://docs.qualcomm.com/pr	H-QUA-WCD9-200125/710

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL calls. **CVE ID: CVE-2024-33059**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/711
Product: wcd9390					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/712
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/713
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/714
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/715
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls.	https://docs.qualcomm.com/product/publicres	H-QUA-WCD9-200125/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33059	ources/security bulletin/january -2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/717
Product: wcd9395					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/718
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/719
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/720
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/721
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers.	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WCD9-200125/722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33055	bulletin/january-2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCD9-200125/723
Product: wcn3620					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/724
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/725
Product: wcn3660b					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/726
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/727
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qualcomm.com/pr	H-QUA-WCN3-200125/728

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
			function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	oduct/publicresources/security bulletin/january-2025-bulletin.html	
Product: wcn3680b					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/729
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/730
Product: wcn3950					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/731
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/732
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/security bulletin/january	H-QUA-WCN3-200125/733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/734
Product: wcn3980					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/735
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/736
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/737
Product: wcn3988					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/739
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/740
Product: wcn3990					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN3-200125/741
Product: wcn6450					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/742
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/743

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45558		
Product: wcn6650					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/744
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/745
Product: wcn6740					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/746
Product: wcn6755					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN6-200125/747
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the	https://docs.qualcomm.com/pr	H-QUA-WCN6-200125/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: wcn7860					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/749
Product: wcn7861					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/750
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/751
Product: wcn7880					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcn7881					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/753
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WCN7-200125/754
Product: wsa8810					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/755
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/756
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/757
Stack-based	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	H-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/758
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/759
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/760
Product: wsa8815					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/761
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/762
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/763
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-WSA8-200125/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/765
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/766
Product: wsa8830					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/767
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/768
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/769
Buffer Copy	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	H-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/770
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/771
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/772
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/773
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/774
Product: wsa8832					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/775
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-WSA8-200125/776

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/777
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/778
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/779
Product: wsa8835					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/780
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/781
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-WSA8-200125/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/783
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/784
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/785
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/786
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/787
Product: wsa8840					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-WSA8-200125/788

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/789
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/791
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/792
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/793
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/794
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS	https://docs.qualcomm.com/product/publicresources/security	H-QUA-WSA8-200125/795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			encryption and decryption functionality. **CVE ID: CVE-2024-45547**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/796
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/797
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/798
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/799
Product: wsa8845					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/800
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/801
Improper	06-Jan-2025	7.8	Memory corruption occurs	https://docs.qu	H-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/802
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/803
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/805
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/806
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/807
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	H-QUA-WSA8-200125/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/809
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/810
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/811
Product: wsa8845h					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/812
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/813
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-WSA8-200125/814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/815
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/816
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/817
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/818
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/819
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/820
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	H-QUA-WSA8-200125/821

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33041	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/822
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	H-QUA-WSA8-200125/823
Operating System					
Vendor: Fortinet					
Product: fortios					
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.0.17					
Authentication Bypass Using an Alternate Path or Channel	14-Jan-2025	9.8	An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS version 7.0.0 through 7.0.16 and FortiProxy version 7.0.0 through 7.0.19 and 7.2.0 through 7.2.12 allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module. **CVE ID: CVE-2024-55591**	https://fortiguard.fortinet.com/psirt/FG-IR-24-535	O-FOR-FORT-200125/824
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	08-Jan-2025	7.8	In DevmemIntMapPages of devicemem_server.c, there is a possible physical page uaf due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges	N/A	O-GOO-ANDR-200125/825

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. **CVE ID: CVE-2023-35685**		
Vendor: Huawei					
Product: emui					
Affected Version(s): 12.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/826
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/827
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/828
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/829
Improper Limitation of a Pathname to a	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			vulnerability will affect integrity and confidentiality. **CVE ID: CVE-2023-52953**		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56442**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/831
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/832
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/833
Affected Version(s): 13.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/834
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/835

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			availability. **CVE ID: CVE-2024-56448**		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/836
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/837
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. **CVE ID: CVE-2023-52953**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/838
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56440**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/839
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56442**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/840

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
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/841
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/842
Affected Version(s): 14.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/843
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/844
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/845
Buffer Copy without Checking	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module	https://consumer.huawei.com/en/support/bull	O-HUA-EMUI-200125/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56450**	etin/2025/1/	
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56440**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/847
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56438**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/848
Operation on a Resource after Expiration or Release	08-Jan-2025	4.4	UAF vulnerability in the device node access module Impact: Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID: CVE-2024-56434**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/849
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-EMUI-200125/850
Product: harmonyos					
Affected Version(s): 2.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/852
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/853
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/854
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. **CVE ID: CVE-2023-52953**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/855
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56442		
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/857
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/858
Affected Version(s): 2.1.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/859
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/860
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/861
N/A	08-Jan-2025	6.5	Vulnerability of improper	https://consum	O-HUA-HARM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	er.huawei.com/en/support/bulletin/2025/1/	200125/862
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. **CVE ID: CVE-2023-52953**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/863
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56442**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/864
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/865
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/866
Affected Version(s): 3.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management	https://consumer.huawei.com/en/support/bull	O-HUA-HARM-200125/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	etin/2025/1/	
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/868
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/869
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/870
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Jan-2025	6.2	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality. **CVE ID: CVE-2023-52953**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/871
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			abnormally. **CVE ID: CVE-2024-56440**		
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56442**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/873
N/A	08-Jan-2025	4.4	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/874
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/875
Affected Version(s): 3.1.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/876
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/877

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-56448		
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/878
N/A	08-Jan-2025	6.5	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2023-52955**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/879
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56440**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/880
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56438**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/881
N/A	08-Jan-2025	5.5	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56442**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/882
N/A	08-Jan-2025	4.4	Vulnerability of improper	https://consum	O-HUA-HARM-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2023-52954**	er.huawei.com/en/support/bulletin/2025/1/	200125/883
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/884
Affected Version(s): 4.0.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56447**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/885
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/886
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/887
Buffer Copy without Checking Size of Input	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module Impact: Successful	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56450**		
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56440**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/889
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56438**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/890
Operation on a Resource after Expiration or Release	08-Jan-2025	4.4	UAF vulnerability in the device node access module Impact: Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID: CVE-2024-56434**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/891
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/892
Affected Version(s): 4.2.0					
Improper Privilege Management	08-Jan-2025	7.8	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service confidentiality. **CVE ID: CVE-2024-56447**		
Improper Control of Generation of Code ('Code Injection')	08-Jan-2025	6.7	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56448**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/894
N/A	08-Jan-2025	6.6	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56449**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	6.3	Buffer overflow vulnerability in the component driver module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56450**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/896
N/A	08-Jan-2025	6.2	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56440**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/897
N/A	08-Jan-2025	6	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56438**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/898
Operation on a	08-Jan-2025	4.4	UAF vulnerability in the device node access module	https://consumer.huawei.com/	O-HUA-HARM-200125/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource after Expiration or Release			Impact: Successful exploitation of this vulnerability may cause service exceptions of the device. **CVE ID: CVE-2024-56434**	en/support/bulletin/2025/1/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56441**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/900
Affected Version(s): 5.0.0					
Protection Mechanism Failure	08-Jan-2025	7.5	Access control vulnerability in the identity authentication module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56439**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/901
N/A	08-Jan-2025	7.5	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56444**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/902
Integer Overflow to Buffer Overflow	08-Jan-2025	7.3	Integer overflow vulnerability during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56451**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/903
Buffer Copy without Checking Size of Input ('Classic	08-Jan-2025	6.8	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/904

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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')			Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56456**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	6.8	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56453**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/905
Improper Input Validation	08-Jan-2025	6.2	Startup control vulnerability in the ability module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-54121**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/906
Exposure of Sensitive Information to an Unauthorized Actor	08-Jan-2025	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56443**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/907
Exposure of Sensitive Information to an Unauthorized Actor	08-Jan-2025	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56435**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/908
Improper Input Validation	08-Jan-2025	5.7	Vulnerability of input parameters not being verified in the widget framework module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect availability. **CVE ID: CVE-2024-56437**		
N/A	08-Jan-2025	5.5	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID: CVE-2024-56436**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56455**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/911
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56454**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/912
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Jan-2025	5.5	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56452**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/913
Improper Authentication	08-Jan-2025	4.3	Instruction authentication bypass vulnerability in the Findnetwork module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-56445**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-Jan-2025	4.1	Race condition vulnerability in the distributed notification module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID: CVE-2024-54120**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/915
Use of Uninitialized Variable	08-Jan-2025	4	Vulnerability of variables not being initialized in the notification module Impact: Successful exploitation of this vulnerability may affect availability. **CVE ID: CVE-2024-56446**	https://consumer.huawei.com/en/support/bulletin/2025/1/	O-HUA-HARM-200125/916
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 4.9.333					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/917
Affected Version(s): * Up to (excluding) 5.10.231					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/01575f2ff8ba578a3436f230668	O-LIN-LINU-200125/918

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
			MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0 Missing '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which	bd056dc2eb823, https://git.kernel.org/stable/c/4fbd66d8254cedfd1218393f39d83b6c07a01917, https://git.kernel.org/stable/c/5a2eaa3ad2b803c7ea442c6db7379466ee73c024	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 fixed the issue for ls2k (despite its subject mentions ls7a). **CVE ID: CVE-2024-56785**		
Affected Version(s): * Up to (excluding) 5.15.174					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns -EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. " ----------[cut here]----------	https://git.kernel.org/stable/c/2129f6faa5dfe8c6b87aad11720bf75edd77d3e4, https://git.kernel.org/stable/c/997a3c04d7fa3d1d385c14691350d096fada648c, https://git.kernel.org/stable/c/9cc832d37799dbea950c4c8a34721b02b8b5a8ff	O-LIN-LINU-200125/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARNING: CPU: 1 PID: 1 at drivers/soc/imx/soc-imx8m.c:115 imx8mm_soc_revision+0xdc/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924-00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : imx8mm_soc_revision+0xdc/0x180 lr : imx8mm_soc_revision+0xd0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbce0 x28: 0000000000000000 x27: ffff800081810120 x26: ffff8000818a9970 x25: 0000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffdfb x20: ffff800082780000 x19: 0000000000000001 x18: ffffffffffffffff x17: ffff800081fff418 x16: ffff8000823e1000 x15: ffff0000c03b65e8 x14: ffff0000c00051b0 x13: ffff800082790000 x12: 0000000000000801 x11: ffff80008278ffff x10: ffff80008209d3a6 x9 : ffff80008062e95c x8 : ffff8000821fb9a0 x7 : 0000000000000000 x6 : 00000000000080e3 x5 : ffff0000df8c03d8 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			: ffffffffffffdfb x0 : ffffffffffffdfb Call trace: imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- SoC: i.MX8MP revision 1.1 " **CVE ID: CVE-2024-56787**		
Affected Version(s): * Up to (excluding) 5.4.287					
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kernel.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	O-LIN-LINU-200125/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			_nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */ rpc_run_task rpc_wait_for_completion_task While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak. Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateowner // alloc oo1, stateid1 nfsd4_open nfsd4_process_open1 find_or_alloc_open_stateowner // find oo1, without NFS4_OO_CONFIRMED release_openowner unhash_openowner_locked list_del_init(&oo->oo_perclient) // cannot find this oo // from client, LEAK!!! alloc_stateowner // alloc oo2 nfsd4_process_open2 init_open_stateid // associate oo1 // with stateid1, stateid1 LEAK!!! nfs4_get_vfs_file // alloc nfsd_file1 and nfsd_file_mark1 // all LEAK!!! nfsd4_process_open2 ... write_threads		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			...
			
			nfsd_destroy_serv
			
			nfsd_shutdown_net
			
			nfs4_state_shutdown_net
			
			nfs4_state_destroy_net
			
			destroy_client
			
			__destroy_client
			//
			won't find oo1!!!
			
			nfsd_shutdown_generic
			
			nfsd_file_cache_shutdown
			
			kmem_cache_destroy
			for
			nfsd_file_slab
			and
			nfsd_file_mark_slab
			// bark
			since nfsd_file1
			// and
			nfsd_file_mark1
			// still
			alive
			
			==========
			==========
			==========
			========
			BUG nfsd_file (Not tainted):
			Objects remaining in
			nfsd_file on
			__kmem_cache_shutdown()
			---------- 	
			---------- 	
			
			Slab 0xffd4000004438a80
			objects=34 used=1
			fp=0xff11000110e2ad28
			flags=0x17ffffc0000240(wo
			rkingset|head|node=0|zone
			=2|lastcpupid=0x1fffff)
			CPU: 4 UID: 0 PID: 757
			Comm: sh Not tainted
			6.12.0-rc6+ #19		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x2	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling") **CVE ID: CVE-2024-56781**		
Affected Version(s): * Up to (excluding) 6.12.4					
Missing Release of Memory after Effective Lifetime	08-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix handling of plane refcount [Why] The mechanism to backup and restore plane states doesn't maintain refcount, which can cause issues if the refcount of the plane changes in between backup and	https://git.kernel.org/stable/c/27227a234c1487cb7a684615f0749c455218833a, https://git.kernel.org/stable/c/8cb2f6793845f135b28361ba8e96901cae3e5790	O-LIN-LINU-200125/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			restore operations, such as memory leaks if the refcount was supposed to go down, or double frees / invalid memory accesses if the refcount was supposed to go up. [How] Cache and re-apply current refcount when restoring plane states. **CVE ID: CVE-2024-56775**		
Affected Version(s): * Up to (excluding) 6.12.5					
Out-of-bounds Write	08-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adding array index check to prevent memory corruption [Why & How] Array indices out of bound caused memory corruption. Adding checks to ensure that array index stays in bound. **CVE ID: CVE-2024-56784**	https://git.kernel.org/stable/c/2c437d9a0b496168e1a1defd17b531f0a526dbe9, https://git.kernel.org/stable/c/dff526dc3e27f5484f5ba11471b9fbbe681467f2	O-LIN-LINU-200125/923
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: ACPI: x86: Add adev NULL check to acpi_quirk_skip_serdev_enumeration() acpi_dev_hid_match() does not check for adev == NULL, dereferencing it unconditional. Add a check for adev being NULL before calling acpi_dev_hid_match(). At the moment acpi_quirk_skip_serdev_enu	https://git.kernel.org/stable/c/4a49194f587a62d972b602e3e1a2c3cfe6567966, https://git.kernel.org/stable/c/e173bce05f7032a8b4964cfef82a4b7668f5f3af	O-LIN-LINU-200125/924

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			meration() is never called with a controller_parent without an ACPI companion, but better safe than sorry. **CVE ID: CVE-2024-56782**		
Affected Version(s): * Up to (excluding) 6.12.8					
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we have the tracepoint trace_btrfs_cow_block() enabled and preemption is also enabled (CONFIG_PREEMPT=y), we can trigger a use-after-free in the COWed extent buffer while inside the tracepoint code. This is because in some paths that call btrfs_cow_block(), such as btrfs_search_slot(), we are holding the last reference on the extent buffer @buf so btrfs_force_cow_block() drops the last reference on the @buf extent buffer when it calls free_extent_buffer_stale(buf), which schedules the release of the extent buffer with RCU. This means that if we are on a kernel with preemption, the current task may be preempted before calling trace_btrfs_cow_block() and the extent buffer already released by the time trace_btrfs_cow_block() is called, resulting in a use-	https://git.kernel.org/stable/c/44f52bbe96dfdbe4aca3818a2534520082a07040, https://git.kernel.org/stable/c/c3a403d8ce36f5a809a492581de5ad17843e4701	O-LIN-LINU-200125/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			after-free. Fix this by moving the trace_btrfs_cow_block() from btrfs_cow_block() to btrfs_force_cow_block() before the COWed extent buffer is freed. This also has a side effect of invoking the tracepoint in the tree defrag code, at defrag.c:btrfs_realloc_node( ), since btrfs_force_cow_block() is called there, but this is fine and it was actually missing there. **CVE ID: CVE-2024-56759**		
Improper Resource Shutdown or Release	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: mediatek: add intf release flow when usb disconnect MediaTek claim an special usb intr interface for ISO data transmission. The interface need to be released before unregistering hci device when usb disconnect. Removing BT usb dongle without properly releasing the interface may cause Kernel panic while unregister hci device. **CVE ID: CVE-2024-56757**	https://git.kernel.org/stable/c/489304e67087abddc2666c5af0159cb95afdcf59, https://git.kernel.org/stable/c/cc569d791ab2a0de74f76e470515d25d24c9b84b	O-LIN-LINU-200125/926
Affected Version(s): * Up to (excluding) 6.6.66					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: put bpf_link's program when link is safe to be deallocated	https://git.kernel.org/stable/c/2fcb921c2799c49ac5e365cf4110f94a64ae4885, https://git.kernel.org/stable/c/	O-LIN-LINU-200125/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In general, BPF link's underlying BPF program should be considered to be reachable through attach hook -> link -> prog chain, and, pessimistically, we have to assume that as long as link's memory is not safe to free, attach hook's code might hold a pointer to BPF program and use it. As such, it's not (generally) correct to put link's program early before waiting for RCU GPs to go through. More eager bpf_prog_put() that we currently do is mostly correct due to BPF program's release code doing similar RCU GP waiting, but as will be shown in the following patches, BPF program can be non-sleepable (and, thus, reliant on only "classic" RCU GP), while BPF link's attach hook can have sleepable semantics and needs to be protected by RCU Tasks Trace, and for such cases BPF link has to go through RCU Tasks Trace + "classic" RCU GPs before being deallocated. And so, if we put BPF program early, we might free BPF program before we free BPF link, leading to use-after-free situation. So, this patch defers bpf_prog_put() until we are ready to perform bpf_link's deallocation. At worst, this delays BPF program freeing by	5fe23c57abadfd46a7a66e81f3536e4757252a0b, https://git.kernel.org/stable/c/f44ec8733a8469143fde1984b5e6931b2e2f6f3f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			one extra RCU GP, but that seems completely acceptable. Alternatively, we'd need more elaborate ways to determine BPF hook, BPF link, and BPF program lifetimes, and how they relate to each other, which seems like an unnecessary complication. Note, for most BPF links we still will perform eager bpf_prog_put() and link dealloc, so for those BPF links there are no observable changes whatsoever. Only BPF links that use deferred dealloc might notice slightly delayed freeing of BPF programs. Also, to reduce code and logic duplication, extract program put + link dealloc logic into bpf_link_dealloc() helper. **CVE ID: CVE-2024-56786**		
Affected Version(s): 6.1					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/928
Affected Version(s): 6.13					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries	https://git.kernel.org/stable/c/05aa156e156ef3168e7ab8a68721945196495c17, https://git.kernel.org/stable/c/6d9cd27105459f169993a4c5f216499a946dbf34, https://git.kernel.org/stable/c/8b2282b5084521254a2cd9742a3f4e1d5b77f843	O-LIN-LINU-200125/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c0000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c0000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c0000000006eb5c8] __asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c00000000013f898] reconfig_close_windows+0x1a0/0x4e8 [16386.255343] [c00000016b297990] [c000000000140e58] vas_migration_handler+0x3a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0x4c/0x4c4 ... [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x68 [16386.256163] kasan_save_track+0x34/0x80 [16386.256175] kasan_save_alloc_info+0x58/0x74 [16386.256196] __kasan_slab_alloc+0xb8/0xdc [16386.256209] kmem_cache_alloc_noprof+		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x24c [16386.256292] ksys_mmap_pgoff+0x20c/0x348 [16386.256303] sys_mmap+0xd0/0x160 ... [16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x68 [16386.256374] kasan_save_track+0x34/0x80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396] __kasan_slab_free+0x120/0x204 [16386.256415] kmem_cache_free+0x128/0x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x60c [16386.256495] do_softirq_own_stack+0x6c/0x88 [16386.256509] do_softirq_own_stack+0x58/0x88		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256521] __irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepare.constprop.0+0x18/0x2c ... [16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x68 [16386.256741] __kasan_record_aux_stack+0xcc/0x12c [16386.256753] __call_rcu_common.constprop.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.constprop.0+0x684/0x870 [16386.256811] __vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a0/0x4a0 [16386.256841] system_call_vectored_common+0x15c/0x2ec [16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14a81 [16386.256950] memcg:c0000000ba430001 [16386.256961] anon flags: 0x43ffff800000000(node=4|zone=0|lastcpupid=0x7ffff) [16386.256975] page_type: 0xfdffffff(slab) [16386 ---truncated--- **CVE ID: CVE-2024-56765**		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ublk: detach gendisk from ublk device if add_disk() fails Inside ublk_abort_requests(), gendisk is grabbed for aborting all inflight requests. And ublk_abort_requests() is called when exiting the uring context or handling timeout. If add_disk() fails, the gendisk may have been freed when calling ublk_abort_requests(), so use-after-free can be caused when getting disk's reference in ublk_abort_requests(). Fixes the bug by detaching gendisk from ublk device if add_disk() fails.	https://git.kernel.org/stable/c/75cd4005da5492129917a4a4ee45e816605561 04, https://git.kernel.org/stable/c/7d680f2f76a3417fdfc3946da7471e81464f7b41	O-LIN-LINU-200125/930

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-56764		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we have the tracepoint trace_btrfs_cow_block() enabled and preemption is also enabled (CONFIG_PREEMPT=y), we can trigger a use-after-free in the COWed extent buffer while inside the tracepoint code. This is because in some paths that call btrfs_cow_block(), such as btrfs_search_slot(), we are holding the last reference on the extent buffer @buf so btrfs_force_cow_block() drops the last reference on the @buf extent buffer when it calls free_extent_buffer_stale(buf), which schedules the release of the extent buffer with RCU. This means that if we are on a kernel with preemption, the current task may be preempted before calling trace_btrfs_cow_block() and the extent buffer already released by the time trace_btrfs_cow_block() is called, resulting in a use-after-free. Fix this by moving the trace_btrfs_cow_block() from btrfs_cow_block() to btrfs_force_cow_block()	https://git.kernel.org/stable/c/44f52bbe96dfdbe4aca3818a2534520082a07040, https://git.kernel.org/stable/c/c3a403d8ce36f5a809a492581de5ad17843e4701	O-LIN-LINU-200125/931

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before the COWed extent buffer is freed. This also has a side effect of invoking the tracepoint in the tree defrag code, at defrag.c:btrfs_realloc_node( ), since btrfs_force_cow_block() is called there, but this is fine and it was actually missing there. **CVE ID: CVE-2024-56759**		
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/932
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values.	https://git.kernel.org/stable/c/1d6de21f00293d819b5ca6dbe75ff1f3b6392140, https://git.kernel.org/stable/c/2dd59fe0e19e1ab955259978082b62e5751924c7, https://git.kernel.org/stable/c/3876e3a1c31a58a352c6bf5d2a90e3304445a637	O-LIN-LINU-200125/933

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem. [1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ========== ========== ========== BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dibusb_dib3000mb_frontend_attach+0x155/0x2f0 drivers/media/usb/dvb-usb/dibusb-mb.c:31 dvb_usb_adapter_frontend_init+0xed/0x9a0 drivers/media/usb/dvb-usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:186 [inline] dvb_usb_device_init+0x25a8/0x3760 drivers/media/usb/dvb-usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb-usb/dibusb-mb.c:110 ... Local variable rb created at:		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dib3000_read_reg+0x86/0x4e0 drivers/media/dvb-frontends/dib3000mb.c:54 dib3000mb_attach+0x123/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 ... **CVE ID: CVE-2024-56769**		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_get_smp_processor_id() on !CONFIG_SMP On x86-64 calling bpf_get_smp_processor_id() in a kernel with CONFIG_SMP disabled can trigger the following bug, as pcpu_hot is unavailable: [8.471774] BUG: unable to handle page fault for address: 00000000936a290c [8.471849] #PF: supervisor read access in kernel mode [8.471881] #PF: error_code(0x0000) - not-present page Fix by inlining a return 0 in the !CONFIG_SMP case. **CVE ID: CVE-2024-56768**	https://git.kernel.org/stable/c/23579010cf0a12476e96a5f1acdf78a9c5843657, https://git.kernel.org/stable/c/f4ab7d74247b0150547cf909b3f6f24ee85183df	O-LIN-LINU-200125/934
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memset	https://git.kernel.org/stable/c/54376d8d26596f98ed7432a788314bb9154bf3e3, https://git.kernel.org/stable/c/c43ec96e8d343	O-LIN-LINU-200125/935

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 at_xdmac_memset_create_desc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. **CVE ID: CVE-2024-56767**	99bd9dab2f2dc316b904892133f, https://git.kernel.org/stable/c/e658f1c133b854b2ae799147301d82dddb8f3162	
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. **CVE ID: CVE-2024-56763**	https://git.kernel.org/stable/c/03041e474a6a8f1bfd4b96b164bb3165c48fa1a3, https://git.kernel.org/stable/c/1cca920af19df5dd91254e5ff35e68e911683706, https://git.kernel.org/stable/c/3d15f4c2449558ffe83b4dba30614ef1cd6937c3	O-LIN-LINU-200125/936
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Clear WFE in missing-ENDBRANCH #CPs An indirect branch instruction sets the CPU indirect branch tracker (IBT) into WAIT_FOR_ENDBRANCH (WFE) state and WFE stays asserted across the instruction boundary. When the decoder finds an inappropriate instruction while WFE is set ENDBR, the CPU raises a #CP fault.	https://git.kernel.org/stable/c/b939f108e86b76119428a6fa4e92491e09ac7867, https://git.kernel.org/stable/c/dc81e556f2a017d681251ace21bf06c126d5a192	O-LIN-LINU-200125/937

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 the "kernel IBT no ENDBR" selftest where #CPs are deliberately triggered, the WFE state of the interrupted context needs to be cleared to let execution continue. Otherwise when the CPU resumes from the instruction that just caused the previous #CP, another missing-ENDBRANCH #CP is raised and the CPU enters a dead loop. This is not a problem with IDT because it doesn't preserve WFE and IRET doesn't set WFE. But FRED provides space on the entry stack (in an expanded CS area) to save and restore the WFE state, thus the WFE state is no longer clobbered, so software must clear it. Clear WFE to avoid dead looping in ibt_clear_fred_wfe() and the !ibt_fatal code path when execution is allowed to continue. Clobbering WFE in any other circumstance is a security-relevant bug. [dhansen: changelog rewording] **CVE ID: CVE-2024-56761**		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Handle lack of irqdomain gracefully	https://git.kernel.org/stable/c/a60b990798eb17433d0283788280422b1bd94b18, https://git.kern	O-LIN-LINU-200125/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2c/0x32 __pci_enable_msix_range+0x30c/0x596 pci_msi_setup_msi_irqs+0x2c/0x32 pci_alloc_irq_vectors_affinity+0xb8/0xe2 RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub. That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP. Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are weak implementations which return an error, so the problem was papered	el.org/stable/c/aed157301c659a48f5564cc4568cf0e5c8831af0, https://git.kernel.org/stable/c/b1f7476e07b93d65a1a3643dcb4a7bed80d4328d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			over. Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it. **CVE ID: CVE-2024-56760**		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: 0000 [#1] SMP CPU: 76 PID: 1411631 Comm: kworker/u322:5 Workqueue: events_unbound btrfs_reclaim_bgs_work RIP: 0010:set_page_extent_mapp	https://git.kernel.org/stable/c/3e74859ee35edc33a022c3f3971df066ea0ca6b9, https://git.kernel.org/stable/c/d508e56270389b3a16f5b3cf247f4eb1bbad1578	O-LIN-LINU-200125/939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ed+0x20/0xb0 RSP: 0018:ffffc900516a7be8 EFLAGS: 00010246 RAX: ffffea009e851d08 RBX: ffffea009e0b1880 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffffc900516a7b90 RDI: ffffea009e0b1880 RBP: 0000000003573000 R08: 0000000000000001 R09: ffff88c07fd2f3f0 R10: 0000000000000000 R11: 0000194754b575be R12: 0000000003572000 R13: 0000000003572fff R14: 0000000000100cca R15: 0000000005582fff FS: 0000000000000000(0000) GS:ffff88c07fd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 000000407d00f002 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die+0x78/0xc0 ? page_fault_oops+0x2a8/0x3a0 ? __switch_to+0x133/0x530 ? wq_worker_running+0xa/0x40 ? exc_page_fault+0x63/0x130 ? asm_exc_page_fault+0x22/0x30		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? set_page_extent_mapped+0x20/0xb0 relocate_file_extent_cluster+0x1a7/0x940 relocate_data_extent+0xaf/0x120 relocate_block_group+0x20f/0x480 btrfs_relocate_block_group+0x152/0x320 btrfs_relocate_chunk+0x3d/0x120 btrfs_reclaim_bgs_work+0x2ae/0x4e0 process_scheduled_works+0x184/0x370 worker_thread+0xc6/0x3e0 ? blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork+0x2f/0x40 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork_asm+0x11/0x20 </TASK> This occurs because cleanup_one_transaction() calls destroy_delalloc_inodes() which calls invalidate_inode_pages2() which takes the folio_lock before setting mapping to NULL. We fail to check this, and subsequently call		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode) Note that the "fixes" patch here is not the one that introduced the race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice. **CVE ID: CVE-2024-56758**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.
			
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine
			as follows:
			$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
			$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
			
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics:
			$ tc -s qdisc show dev <oif>
			
			Statistics after 10s of iPerf3 TCP test before the fix (note that
			netem's backlog > limit, netem stopped accepting packets):
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0)
			backlog 4294528236b 1155p requeues 0
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms
			Sent 2767766 bytes 1848 pkt (dropped 327,		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). **CVE ID: CVE-2024-56774**	https://git.kernel.org/stable/c/3ed51857a50f530ac7a1482e069dfbd1298558d4, https://git.kernel.org/stable/c/757171d1369b3b47f36932d40a05a0715496dcab, https://git.kernel.org/stable/c/93992c3d9629b02dccf6849238559d5c24f2dece	O-LIN-LINU-200125/941
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary	https://git.kernel.org/stable/c/2f9bec0a749eb646b384fde0c7b7c24687b2ffae, https://git.kernel.org/stable/c/7064a6daa4a700a298fe3aee11dea296bfe59fc4, https://git.kernel.org/stable/c/b7529880cb961d515642ce63f9d7570869bbbdc3	O-LIN-LINU-200125/942

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WARN_ON_ONCE which is reachable from userspace. **CVE ID: CVE-2024-56783**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4]	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26 , https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	O-LIN-LINU-200125/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 2.6.19 Up to (excluding) 6.1.123					
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values. Since no elaborate error handling is expected in dib3000_write_reg(),	https://git.kernel.org/stable/c/1d6de21f00293d819b5ca6dbe75ff1f3b6392140, https://git.kernel.org/stable/c/2dd59fe0e19e1ab955259978082b62e5751924c7, https://git.kernel.org/stable/c/3876e3a1c31a58a352c6bf5d2a90e3304445a637	O-LIN-LINU-200125/944

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			simply zero out rb buffer to mitigate the problem. [1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ========== ========== ========== BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dibusb_dib3000mb_frontend_attach+0x155/0x2f0 drivers/media/usb/dvb-usb/dibusb-mb.c:31 dvb_usb_adapter_frontend_init+0xed/0x9a0 drivers/media/usb/dvb-usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:186 [inline] dvb_usb_device_init+0x25a8/0x3760 drivers/media/usb/dvb-usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb-usb/dibusb-mb.c:110 ... Local variable rb created at: dib3000_read_reg+0x86/0x4e0 drivers/media/dvb-frontends/dib3000mb.c:54		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dib3000mb_attach+0x123/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 ... **CVE ID: CVE-2024-56769**		
Affected Version(s): From (including) 2.6.29 Up to (excluding) 6.1.123					
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. **CVE ID: CVE-2024-56763**	https://git.kernel.org/stable/c/03041e474a6a8f1bfd4b96b164bb3165c48fa1a3, https://git.kernel.org/stable/c/1cca920af19df5dd91254e5ff35e68e911683706, https://git.kernel.org/stable/c/3d15f4c2449558ffe83b4dba30614ef1cd6937c3	O-LIN-LINU-200125/945
Affected Version(s): From (including) 3.3 Up to (excluding) 5.4.288					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full. Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: $ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 $ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: $ tc -s qdisc show dev <oif> Statistics after 10s of iPerf3 TCP test before the fix (note that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 4.10 Up to (excluding) 4.14.299					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/947
Affected Version(s): From (including) 4.15 Up to (excluding) 4.19.265					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b3	O-LIN-LINU-200125/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				9	
Affected Version(s): From (including) 4.19.295 Up to (excluding) 4.20					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4]	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26, https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	O-LIN-LINU-200125/949

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 4.19.325 Up to (excluding) 4.20					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/950
Affected Version(s): From (including) 4.2 Up to (excluding) 6.1.123					
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memse	https://git.kernel.org/stable/c/54376d8d26596f98ed7432a788314bb9154bf3e3, https://git.kern	O-LIN-LINU-200125/951

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
			t The at_xdmac_memset_create_desc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. **CVE ID: CVE-2024-56767**	el.org/stable/c/c43ec96e8d34399bd9dab2f2dc316b904892133f, https://git.kernel.org/stable/c/e658f1c133b854b2ae799147301d82dddb8f3162	
Affected Version(s): From (including) 4.20 Up to (excluding) 5.4.224					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/952
Affected Version(s): From (including) 4.6 Up to (excluding) 5.15.174					
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure.	https://git.kernel.org/stable/c/40725c5fabee804fecce41d4d5c5bae80c45e1c4, https://git.kernel.org/stable/c/831214f77037de02afc287eae93ce97f218d8c04, https://git.kernel.org/stable/c/8ab73ac97c0fa528f66eeccd9bb53eb6eb7d20dc	O-LIN-LINU-200125/953

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-56776		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56777**	https://git.kernel.org/stable/c/3cf2e7c448e246f7e700c7aa47450d1e27579559, https://git.kernel.org/stable/c/997b64c3f4c1827c5cfda8ae7f5d13f78d28b541, https://git.kernel.org/stable/c/b79612ed6bc1a184c45427105c851b5b2d4342ca	O-LIN-LINU-200125/954
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56778**	https://git.kernel.org/stable/c/31c857e7496d34e5a32a6f75bc024d0b06fd646a, https://git.kernel.org/stable/c/6b0d0d6e9d3c26697230bf7dc9e6b52bdb24086f, https://git.kernel.org/stable/c/82a5312f874fb18f045d9658e9bd290e3b0621c0	O-LIN-LINU-200125/955
Affected Version(s): From (including) 5.10.195 Up to (excluding) 5.10.231					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super()	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26 , https://git.kern	O-LIN-LINU-200125/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.	el.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 5.10.231 Up to (excluding) 5.11					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/957
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.174					
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kernel.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	O-LIN-LINU-200125/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */ rpc_run_task rpc_wait_for_completion_task While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			concurrently, this situation can lead to lots of memory leak.
			Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.
			
			NFS SERVER nfsd1 nfsd2
			echo 0 > /proc/fs/nfsd/threads
			
			nfsd4_open
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// alloc oo1, stateid1
			nfsd4_open
			
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// find oo1, without NFS4_OO_CONFIRMED
			
			release_openowner
			
			unhash_openowner_locked
			
			list_del_init(&oo->oo_perclient)
			// cannot find this oo
			// from client, LEAK!!!
			
			alloc_stateowner // alloc oo2
			
			nfsd4_process_open2
			init_open_stateid
			// associate oo1
			// with stateid1, stateid1 LEAK!!!
			nfs4_get_vfs_file
			// alloc nfsd_file1 and nfsd_file_mark1
			// all LEAK!!!		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			nfsd4_process_open2
			...
			
			write_threads
			...
			
			nfsd_destroy_serv
			
			nfsd_shutdown_net
			
			nfs4_state_shutdown_net
			
			nfs4_state_destroy_net
			
			destroy_client
			
			__destroy_client
			//
			won't find oo1!!!
			
			nfsd_shutdown_generic
			
			nfsd_file_cache_shutdown
			
			kmem_cache_destroy
			for
			nfsd_file_slab
			and
			nfsd_file_mark_slab
			// bark
			since nfsd_file1
			// and
			nfsd_file_mark1
			// still
			alive
			
			==========
			==========
			==========
			========
			BUG nfsd_file (Not tainted):
			Objects remaining in
			nfsd_file on
			__kmem_cache_shutdown()
			---------- 	
			---------- 	
			
			Slab 0xffd4000004438a80
			objects=34 used=1		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fp=0xff11000110e2ad28 flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace:	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling") **CVE ID: CVE-2024-56781**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings:	https://git.kernel.org/stable/c/01575f2ff8ba578a3436f230668bd056dc2eb823, https://git.kernel.org/stable/c/4fbd66d8254ce	O-LIN-LINU-200125/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0 Missing '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a). **CVE ID: CVE-2024-56785**	dfd1218393f39d83b6c07a01917, https://git.kernel.org/stable/c/5a2eaa3ad2b803c7ea442c6db7379466ee73c024	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). **CVE ID: CVE-2024-56774**	https://git.kernel.org/stable/c/3ed51857a50f530ac7a1482e069dfbd1298558d4, https://git.kernel.org/stable/c/757171d1369b3b47f36932d40a05a0715496dcab, https://git.kernel.org/stable/c/93992c3d9629b02dccf6849238559d5c24f2dece	O-LIN-LINU-200125/961
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.175					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full. Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine as follows: $ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100 $ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics: $ tc -s qdisc show dev <oif> Statistics after 10s of iPerf3 TCP test before the fix (note		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that netem's backlog > limit, netem stopped accepting packets): qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.78					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/963
Affected Version(s): From (including) 5.15.132 Up to (excluding) 5.15.174					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is:	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26,	O-LIN-LINU-200125/964

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
			freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on	https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 5.15.174 Up to (excluding) 5.16					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/965
Affected Version(s): From (including) 5.16 Up to (excluding) 6.0.8					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/966
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.120					
NULL Pointer	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has	https://git.kernel.org/stable/c/	O-LIN-LINU-200125/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). **CVE ID: CVE-2024-56774**	3ed51857a50f530ac7a1482e069dfbd1298558d4, https://git.kernel.org/stable/c/757171d1369b3b47f36932d40a05a0715496dcab, https://git.kernel.org/stable/c/93992c3d9629b02dccf6849238559d5c24f2dece	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56776**	https://git.kernel.org/stable/c/40725c5fabee804fecce41d4d5c5bae80c45e1c4, https://git.kernel.org/stable/c/831214f77037de02afc287eae93ce97f218d8c04, https://git.kernel.org/stable/c/8ab73ac97c0fa528f66eeccd9bb53eb6eb7d20dc	O-LIN-LINU-200125/968
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential	https://git.kernel.org/stable/c/3cf2e7c448e246f7e700c7aa47450d1e27579559,	O-LIN-LINU-200125/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56777**	https://git.kernel.org/stable/c/997b64c3f4c1827c5cfda8ae7f5d13f78d28b541, https://git.kernel.org/stable/c/b79612ed6bc1a184c45427105c851b5b2d4342ca	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56778**	https://git.kernel.org/stable/c/31c857e7496d34e5a32a6f75bc024d0b06fd646a, https://git.kernel.org/stable/c/6b0d0d6e9d3c26697230bf7dc9e6b52bdb24086f, https://git.kernel.org/stable/c/82a5312f874fb18f045d9658e9bd290e3b0621c0	O-LIN-LINU-200125/970
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server.	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kernel.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	O-LIN-LINU-200125/971

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
			NFS CLIENT thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */ rpc_run_task rpc_wait_for_completion_task While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			two instances of nfsd can run
			concurrently, this situation can lead to lots of memory leak.
			Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.
			
			NFS SERVER nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads
			
			nfsd4_open
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// alloc oo1, stateid1
			nfsd4_open
			
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// find oo1, without NFS4_OO_CONFIRMED
			
			release_openowner
			
			unhash_openowner_locked
			
			list_del_init(&oo->oo_perclient)
			// cannot find this oo
			// from client, LEAK!!!
			
			alloc_stateowner // alloc oo2
			
			nfsd4_process_open2
			init_open_stateid
			// associate oo1
			// with stateid1, stateid1 LEAK!!!
			nfs4_get_vfs_file
			// alloc nfsd_file1 and		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nfsd_file_mark1 // all LEAK!!! nfsd4_process_open2 ... write_threads ... nfsd_destroy_serv nfsd_shutdown_net nfs4_state_shutdown_net nfs4_state_destroy_net destroy_client __destroy_client // won't find oo1!!! nfsd_shutdown_generic nfsd_file_cache_shutdown kmem_cache_destroy for nfsd_file_slab and nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive ========== ========== ========== ======== BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on __kmem_cache_shutdown() ---------- ----------		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28 flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ...	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/972

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling") **CVE ID: CVE-2024-56781**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a	https://git.kernel.org/stable/c/01575f2ff8ba578a3436f230668bd056dc2eb823, https://git.kern	O-LIN-LINU-200125/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix the dtc warnings: arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0 Missing '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a).	el.org/stable/c/4fbd66d8254cedfd1218393f39d83b6c07a01917, https://git.kernel.org/stable/c/5a2eaa3ad2b803c7ea442c6db7379466ee73c024	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56785		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns -EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. " ------------[cut here]------------ WARNING: CPU: 1 PID: 1 at drivers/soc/imx/soc-imx8m.c:115 imx8mm_soc_revision+0xdc	https://git.kernel.org/stable/c/2129f6faa5dfe8c6b87aad11720bf75edd77d3e4, https://git.kernel.org/stable/c/997a3c04d7fa3d1d385c14691350d096fada648c, https://git.kernel.org/stable/c/9cc832d37799dbea950c4c8a34721b02b8b5a8ff	O-LIN-LINU-200125/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924-00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : imx8mm_soc_revision+0xdc /0x180 lr : imx8mm_soc_revision+0xd0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbce0 x28: 0000000000000000 x27: ffff800081810120 x26: ffff8000818a9970 x25: 0000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffdfb x20: ffff800082780000 x19: 0000000000000001 x18: ffffffffffffffff x17: ffff800081fff418 x16: ffff8000823e1000 x15: ffff0000c03b65e8 x14: ffff0000c00051b0 x13: ffff800082790000 x12: 0000000000000801 x11: ffff80008278ffff x10: ffff80008209d3a6 x9 : ffff80008062e95c x8 : ffff8000821fb9a0 x7 : 0000000000000000 x6 : 00000000000080e3 x5 : ffff0000df8c03d8 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1 : fffffffffffffdfb x0 : fffffffffffffdfb 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
			imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- SoC: i.MX8MP revision 1.1 " **CVE ID: CVE-2024-56787**		
Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.121					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.
			
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine
			as follows:
			$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
			$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
			
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics:
			$ tc -s qdisc show dev <oif>
			
			Statistics after 10s of iPerf3 TCP test before the fix (note that
			netem's backlog > limit, netem stopped accepting packets):
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0)
			backlog 4294528236b 1155p requeues 0
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maximum number of packets in the tfifo. The same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 5.18 Up to (excluding) 6.1.123					
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted:	https://git.kernel.org/stable/c/05aa156e156ef3168e7ab8a68721945196495c17, https://git.kernel.org/stable/c/6d9cd27105459f169993a4c5f216499a946dbf34, https://git.kernel.org/stable/c/8b2282b5084521254a2cd9742a3f4e1d5b77f843	O-LIN-LINU-200125/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c0000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c0000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c0000000006eb5c8] __asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c00000000013f898] reconfig_close_windows+0x1a0/0x4e8 [16386.255343] [c00000016b297990] [c000000000140e58] vas_migration_handler+0x3a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0x4c/0x4c4 ... [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x68 [16386.256163] kasan_save_track+0x34/0x80		

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
			[16386.256175] kasan_save_alloc_info+0x58/0x74 [16386.256196] __kasan_slab_alloc+0xb8/0xdc [16386.256209] kmem_cache_alloc_noprof+0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x24c [16386.256292] ksys_mmap_pgoff+0x20c/0x348 [16386.256303] sys_mmap+0xd0/0x160 ... [16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x68 [16386.256374] kasan_save_track+0x34/0x80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396] __kasan_slab_free+0x120/0x204 [16386.256415] kmem_cache_free+0x128/0x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle_softirqs+0x20c/0x60c [16386.256495] do_softirq_own_stack+0x6c/0x88 [16386.256509] do_softirq_own_stack+0x58/0x88 [16386.256521] __irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepare.constprop.0+0x18/0x2c ... [16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x68 [16386.256741] __kasan_record_aux_stack+0xcc/0x12c [16386.256753] __call_rcu_common.constprop.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.constprop.0+0x684/0x870 [16386.256811] __vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a0/0x4a0 [16386.256841] system_call_vectored_common+0x15c/0x2ec [16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14a81 [16386.256950] memcg:c0000000ba430001 [16386.256961] anon flags: 0x43ffff800000000(node=4|zone=0|lastcpupid=0x7ffff) [16386.256975] page_type: 0xfdffffff(slab) [16386 ---truncated--- **CVE ID: CVE-2024-56765**		
Affected Version(s): From (including) 5.4.257 Up to (excluding) 5.4.287					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26, https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	O-LIN-LINU-200125/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.4.287 Up to (excluding) 5.5					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/978
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.154					
Allocation of Resources Without Limits or Throttling	02-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case. **CVE ID: CVE-2022-49035**	https://git.kernel.org/stable/c/1609231f86760c1f6a429de7913dd795b9faa08c, https://git.kernel.org/stable/c/2654e785bd4aa2439cdffbe7dc1ea30a0eddbfe4, https://git.kernel.org/stable/c/4a449430ecfb199b99ba58af63c467eb53500b39	O-LIN-LINU-200125/979
Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.231					
Missing Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kern	O-LIN-LINU-200125/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */ rpc_run_task rpc_wait_for_completion_task While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as	el.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run
			concurrently, this situation can lead to lots of memory leak.
			Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.
			
			NFS SERVER
			nfsd1 nfsd2
			echo 0 > /proc/fs/nfsd/threads
			
			nfsd4_open
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// alloc oo1, stateid1
			nfsd4_open
			
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// find oo1, without
			NFS4_OO_CONFIRMED
			
			release_openowner
			
			unhash_openowner_locked
			
			list_del_init(&oo->oo_perclient)
			// cannot find this oo
			// from client, LEAK!!!
			
			alloc_stateowner // alloc oo2		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			nfsd4_process_open2
			init_open_stateid
			// associate oo1
			// with stateid1, stateid1 LEAK!!!
			nfs4_get_vfs_file
			// alloc nfsd_file1 and nfsd_file_mark1
			// all LEAK!!!
			
			nfsd4_process_open2
			...
			
			write_threads
			...
			
			nfsd_destroy_serv
			
			nfsd_shutdown_net
			
			nfs4_state_shutdown_net
			
			nfs4_state_destroy_net
			
			destroy_client
			
			__destroy_client
			// won't find oo1!!!
			
			nfsd_shutdown_generic
			
			nfsd_file_cache_shutdown
			
			kmem_cache_destroy for nfsd_file_slab
			and nfsd_file_mark_slab
			// bark since nfsd_file1
			// and nfsd_file_mark1
			// still alive
			
			==========
			==========
			==========
			========		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 nfsd_file (Not tainted): Objects remaining in nfsd_file on __kmem_cache_shutdown() --- --- Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28 flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling") **CVE ID: CVE-2024-56781**		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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) 5.10.232					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full. Reproduce the bug: Ensure that the sender machine has GSO enabled.	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/982

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine
			as follows:
			$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
			$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
			
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics:
			$ tc -s qdisc show dev <oif>
			
			Statistics after 10s of iPerf3 TCP test before the fix (note that
			netem's backlog > limit, netem stopped accepting packets):
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0)
			backlog 4294528236b 1155p requeues 0
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms
			Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0)
			backlog 0b 0p requeues 0
			
			Statistics after the fix:
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0)
			backlog 0b 0p requeues 0
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms
			Sent 37766372 bytes		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 6.1.112 Up to (excluding) 6.1.120					
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is	https://git.kernel.org/stable/c/2f9bec0a749eb646b384fde0c7b7c24687b2ffae, https://git.kernel.org/stable/c/7064a6daa4a700a298fe3aee11d	O-LIN-LINU-200125/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is reachable from userspace. **CVE ID: CVE-2024-56783**	ea296bfe59fc4, https://git.kernel.org/stable/c/b7529880cb961d515642ce63f9d7570869bbbdc3	
Affected Version(s): From (including) 6.1.120 Up to (excluding) 6.1.123					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/984
Affected Version(s): From (including) 6.1.53 Up to (excluding) 6.1.120					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26, https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	O-LIN-LINU-200125/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-56780		
Affected Version(s): From (including) 6.1.54 Up to (excluding) 6.2					
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: 0000 [#1] SMP CPU: 76 PID: 1411631 Comm: kworker/u322:5 Workqueue: events_unbound btrfs_reclaim_bgs_work RIP: 0010:set_page_extent_mapped+0x20/0xb0 RSP: 0018:ffffc900516a7be8 EFLAGS: 00010246 RAX: ffffea009e851d08 RBX: ffffea009e0b1880 RCX: 0000000000000000 RDX: 0000000000000000	https://git.kernel.org/stable/c/3e74859ee35edc33a022c3f3971df066ea0ca6b9, https://git.kernel.org/stable/c/d508e56270389b3a16f5b3cf247f4eb1bbad1578	O-LIN-LINU-200125/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSI: ffffc900516a7b90 RDI: ffffea009e0b1880 RBP: 0000000003573000 R08: 0000000000000001 R09: ffff88c07fd2f3f0 R10: 0000000000000000 R11: 0000194754b575be R12: 0000000003572000 R13: 0000000003572fff R14: 0000000000100cca R15: 0000000005582fff FS: 0000000000000000(0000) GS:ffff88c07fd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 000000407d00f002 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die+0x78/0xc0 ? page_fault_oops+0x2a8/0x3a0 ? __switch_to+0x133/0x530 ? wq_worker_running+0xa/0x40 ? exc_page_fault+0x63/0x130 ? asm_exc_page_fault+0x22/0x30 ? set_page_extent_mapped+0x20/0xb0 relocate_file_extent_cluster+0x1a7/0x940 relocate_data_extent+0xaf/		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0x120 relocate_block_group+0x20f /0x480 btrfs_relocate_block_group+ 0x152/0x320 btrfs_relocate_chunk+0x3d/ 0x120 btrfs_reclaim_bgs_work+0x 2ae/0x4e0 process_scheduled_works+ 0x184/0x370 worker_thread+0xc6/0x3e0 ? blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0 ? flush_tlb_kernel_range+0x9 0/0x90 ret_from_fork+0x2f/0x40 ? flush_tlb_kernel_range+0x9 0/0x90 ret_from_fork_asm+0x11/0 x20 </TASK> This occurs because cleanup_one_transaction() calls destroy_delalloc_inodes() which calls invalidate_inode_pages2() which takes the folio_lock before setting mapping to NULL. We fail to check this, and subsequently call set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode) Note that the "fixes" patch here is not the one that introduced 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
			race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice. **CVE ID: CVE-2024-56758**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.12.8					
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_get_smp_processor_id() on !CONFIG_SMP On x86-64 calling bpf_get_smp_processor_id() in a kernel with CONFIG_SMP disabled can trigger the following bug, as pcpu_hot is unavailable: [8.471774] BUG: unable to handle page fault for address: 00000000936a290c [8.471849] #PF: supervisor read access in kernel mode [8.471881] #PF: error_code(0x0000) - not-present page Fix by inlining a return 0 in the !CONFIG_SMP case. **CVE ID: CVE-2024-56768**	https://git.kernel.org/stable/c/23579010cf0a12476e96a5f1acdf78a9c5843657, https://git.kernel.org/stable/c/f4ab7d74247b0150547cf909b3f6f24ee85183df	O-LIN-LINU-200125/987
Affected Version(s): From (including) 6.10.12 Up to (excluding) 6.12.5					
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is	https://git.kernel.org/stable/c/2f9bec0a749eb646b384fde0c7b7c24687b2ffae, https://git.kernel.org/stable/c/7064a6daa4a700a298fe3aee11d	O-LIN-LINU-200125/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is reachable from userspace. **CVE ID: CVE-2024-56783**	ea296bfe59fc4, https://git.kernel.org/stable/c/b7529880cb961d515642ce63f9d7570869bbbdc3	
Affected Version(s): From (including) 6.11.11 Up to (excluding) 6.12					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/989
Affected Version(s): From (including) 6.12.2 Up to (excluding) 6.12.8					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/990
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.64					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kernel.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	O-LIN-LINU-200125/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			rpc_run_task
			
			rpc_wait_for_completion_task
			
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak.
			Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.
			
			NFS SERVER
			nfsd1 nfsd2
			echo 0 > /proc/fs/nfsd/threads
			
			nfsd4_open
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// alloc oo1, stateid1
			nfsd4_open
			
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// find oo1, without NFS4_OO_CONFIRMED
			
			release_openowner		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			unhash_openowner_locked
			
			list_del_init(&oo->oo_perclient)
			// cannot find this oo
			// from client, LEAK!!!
			
			alloc_stateowner // alloc oo2
			
			nfsd4_process_open2
			init_open_stateid
			// associate oo1
			// with stateid1, stateid1 LEAK!!!
			nfs4_get_vfs_file
			// alloc nfsd_file1 and nfsd_file_mark1
			// all LEAK!!!
			
			nfsd4_process_open2
			...
			
			write_threads
			...
			
			nfsd_destroy_serv
			
			nfsd_shutdown_net
			
			nfs4_state_shutdown_net
			
			nfs4_state_destroy_net
			
			destroy_client
			
			__destroy_client
			// won't find oo1!!!
			
			nfsd_shutdown_generic
			
			nfsd_file_cache_shutdown
			
			kmem_cache_destroy for nfsd_file_slab		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive ========== ========== ========== ======== BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on __kmem_cache_shutdown() ---------- ---------- Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28 flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using	https://git.kernel.org/stable/c/3ed51857a50f530ac7a1482e069dfbd1298558d4, https://git.kernel.org/stable/c/757171d1369b3b47f36932d40a05a0715496dcab,	O-LIN-LINU-200125/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). **CVE ID: CVE-2024-56774**	https://git.kernel.org/stable/c/93992c3d9629b02dccf6849238559d5c24f2dece	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56776**	https://git.kernel.org/stable/c/40725c5fabee804fecce41d4d5c5bae80c45e1c4, https://git.kernel.org/stable/c/831214f77037de02afc287eae93ce97f218d8c04, https://git.kernel.org/stable/c/8ab73ac97c0fa528f66eeccd9bb53eb6eb7d20dc	O-LIN-LINU-200125/993
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case	https://git.kernel.org/stable/c/31c857e7496d34e5a32a6f75bc024d0b06fd646a, https://git.kernel.org/stable/c/6b0d0d6e9d3c26697230bf7dc9e6b52bdb24086f, https://git.kernel.org/stable/c/82a5312f874fb18f045d9658e9b	O-LIN-LINU-200125/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of the failure. **CVE ID: CVE-2024-56778**	d290e3b0621c0	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56777**	https://git.kernel.org/stable/c/3cf2e7c448e246f7e700c7aa47450d1e27579559, https://git.kernel.org/stable/c/997b64c3f4c1827c5cfda8ae7f5d13f78d28b541, https://git.kernel.org/stable/c/b79612ed6bc1a184c45427105c851b5b2d4342ca	O-LIN-LINU-200125/995
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.66					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name:	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling") **CVE ID: CVE-2024-56781**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/01575f2ff8ba578a3436f230668	O-LIN-LINU-200125/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0 Missing '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which	bd056dc2eb823, https://git.kernel.org/stable/c/4fbd66d8254cedfd1218393f39d83b6c07a01917, https://git.kernel.org/stable/c/5a2eaa3ad2b803c7ea442c6db7379466ee73c024	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has fixed the issue for ls2k (despite its subject mentions ls7a). **CVE ID: CVE-2024-56785**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns -EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. " ------------[cut here]------------ WARNING: CPU: 1 PID: 1 at	https://git.kernel.org/stable/c/2129f6faa5dfe8c6b87aad11720bf75edd77d3e4, https://git.kernel.org/stable/c/997a3c04d7fa3d1d385c14691350d096fada648c, https://git.kernel.org/stable/c/9cc832d37799dbea950c4c8a34721b02b8b5a8ff	O-LIN-LINU-200125/998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drivers/soc/imx/soc-imx8m.c:115 imx8mm_soc_revision+0xdc/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924-00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : imx8mm_soc_revision+0xdc/0x180 lr : imx8mm_soc_revision+0xd0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbce0 x28: 0000000000000000 x27: ffff800081810120 x26: ffff8000818a9970 x25: 0000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffdfb x20: ffff800082780000 x19: 0000000000000001 x18: ffffffffffffffff x17: ffff800081fff418 x16: ffff8000823e1000 x15: ffff0000c03b65e8 x14: ffff0000c00051b0 x13: ffff800082790000 x12: 0000000000000801 x11: ffff80008278ffff x10: ffff80008209d3a6 x9 : ffff80008062e95c x8 : ffff8000821fb9a0 x7 : 0000000000000000 x6 : 00000000000080e3 x5 : ffff0000df8c03d8 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1 : fffffffffffffdfb x0 :		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffffffffffffdfb Call trace: imx8mm_soc_revision+0xdc/0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a8 kernel_init_freeable+0x240/0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- SoC: i.MX8MP revision 1.1 " **CVE ID: CVE-2024-56787**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.67					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/999

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			wrong number of packets in the tfifo.
			If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen' value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated.
			If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.
			
			Reproduce the bug:
			Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine
			as follows:
			$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
			$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
			
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics:
			$ tc -s qdisc show dev <oif>
			
			Statistics after 10s of iPerf3 TCP test before the fix (note that
			netem's backlog > limit, netem stopped accepting packets):
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.69					
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded	https://git.kernel.org/stable/c/05aa156e156ef3168e7ab8a68721945196495c17, https://git.kernel.org/stable/c/6d9cd27105459f169993a4c5f216499a946dbf34, https://git.kernel.org/stable/c/8b2282b5084521254a2cd9742a3f4e1d5b77f843	O-LIN-LINU-200125/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c0000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c0000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c0000000006eb5c8] __asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c00000000013f898] reconfig_close_windows+0x1a0/0x4e8 [16386.255343] [c00000016b297990] [c000000000140e58] vas_migration_handler+0x3a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0x4c/0x4c4 ... [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x68		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256163] kasan_save_track+0x34/0x80 [16386.256175] kasan_save_alloc_info+0x58/0x74 [16386.256196] __kasan_slab_alloc+0xb8/0xdc [16386.256209] kmem_cache_alloc_noprof+0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x24c [16386.256292] ksys_mmap_pgoff+0x20c/0x348 [16386.256303] sys_mmap+0xd0/0x160 ... [16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x68 [16386.256374] kasan_save_track+0x34/0x80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396] __kasan_slab_free+0x120/0x204 [16386.256415] kmem_cache_free+0x128/0x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x60c [16386.256495] do_softirq_own_stack+0x6c/0x88 [16386.256509] do_softirq_own_stack+0x58/0x88 [16386.256521] __irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepare.constprop.0+0x18/0x2c ... [16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x68 [16386.256741] __kasan_record_aux_stack+0xcc/0x12c [16386.256753] __call_rcu_common.constprop.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.constprop.0+0x684/0x870 [16386.256811] __vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a0/0x4a0 [16386.256841] system_call_vectored_common+0x15c/0x2ec [16386.256868] The buggy address belongs to 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
			object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14a81 [16386.256950] memcg:c0000000ba430001 [16386.256961] anon flags: 0x43ffff800000000(node=4|zone=0|lastcpupid=0x7ffff) [16386.256975] page_type: 0xfdffffff(slab) [16386 ---truncated--- **CVE ID: CVE-2024-56765**		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. **CVE ID: CVE-2024-56763**	https://git.kernel.org/stable/c/03041e474a6a8f1bfd4b96b164bb3165c48fa1a3, https://git.kernel.org/stable/c/1cca920af19df5dd91254e5ff35e68e911683706, https://git.kernel.org/stable/c/3d15f4c2449558ffe83b4dba30614ef1cd6937c3	O-LIN-LINU-200125/1001
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/a60b990798eb17433d02837882	O-LIN-LINU-200125/1002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			PCI/MSI: Handle lack of irqdomain gracefully Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2c/0x32 __pci_enable_msix_range+0x30c/0x596 pci_msi_setup_msi_irqs+0x2c/0x32 pci_alloc_irq_vectors_affinity+0xb8/0xe2 RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub. That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP. Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are	80422b1bd94b18, https://git.kernel.org/stable/c/aed157301c659a48f5564cc4568cf0e5c8831af0, https://git.kernel.org/stable/c/b1f7476e07b93d65a1a3643dcb4a7bed80d4328d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			weak implementations which return an error, so the problem was papered over. Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it. **CVE ID: CVE-2024-56760**		
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values. Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem. [1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ========== ========== ========== BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:75	https://git.kernel.org/stable/c/1d6de21f00293d819b5ca6dbe75ff1f3b6392140, https://git.kernel.org/stable/c/2dd59fe0e19e1ab955259978082b62e5751924c7, https://git.kernel.org/stable/c/3876e3a1c31a58a352c6bf5d2a90e3304445a637	O-LIN-LINU-200125/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8 dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dibusb_dib3000mb_frontend_attach+0x155/0x2f0 drivers/media/usb/dvb-usb/dibusb-mb.c:31 dvb_usb_adapter_frontend_init+0xed/0x9a0 drivers/media/usb/dvb-usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:186 [inline] dvb_usb_device_init+0x25a8/0x3760 drivers/media/usb/dvb-usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb-usb/dibusb-mb.c:110 ... Local variable rb created at: dib3000_read_reg+0x86/0x4e0 drivers/media/dvb-frontends/dib3000mb.c:54 dib3000mb_attach+0x123/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 ... **CVE ID: CVE-2024-56769**		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid	https://git.kernel.org/stable/c/54376d8d26596f98ed7432a788314bb9154bf3	O-LIN-LINU-200125/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			null_prt_deref in at_xdmac_prep_dma_memset The at_xdmac_memset_create_desc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. **CVE ID: CVE-2024-56767**	e3, https://git.kernel.org/stable/c/c43ec96e8d34399bd9dab2f2dc316b904892133f, https://git.kernel.org/stable/c/e658f1c133b854b2ae799147301d82dddb8f3162	
Affected Version(s): From (including) 6.4.16 Up to (excluding) 6.5					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26, https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	O-LIN-LINU-200125/1005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 6.5.3 Up to (excluding) 6.6.64					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is:	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26	O-LIN-LINU-200125/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg	, https://git.kernel.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Affected Version(s): From (including) 6.5.4 Up to (excluding) 6.12.8					
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: 0000 [#1] SMP CPU: 76 PID: 1411631 Comm: kworker/u322:5 Workqueue: events_unbound btrfs_reclaim_bgs_work RIP:	https://git.kernel.org/stable/c/3e74859ee35edc33a022c3f3971df066ea0ca6b9, https://git.kernel.org/stable/c/d508e56270389b3a16f5b3cf247f4eb1bbad1578	O-LIN-LINU-200125/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0010:set_page_extent_mapped+0x20/0xb0 RSP: 0018:ffffc900516a7be8 EFLAGS: 00010246 RAX: ffffea009e851d08 RBX: ffffea009e0b1880 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffffc900516a7b90 RDI: ffffea009e0b1880 RBP: 0000000003573000 R08: 0000000000000001 R09: ffff88c07fd2f3f0 R10: 0000000000000000 R11: 0000194754b575be R12: 0000000003572000 R13: 0000000003572fff R14: 0000000000100cca R15: 0000000005582fff FS: 0000000000000000(0000) GS:ffff88c07fd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 000000407d00f002 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die+0x78/0xc0 ? page_fault_oops+0x2a8/0x3a0 ? __switch_to+0x133/0x530 ? wq_worker_running+0xa/0x40 ? exc_page_fault+0x63/0x130 ? asm_exc_page_fault+0x22/0		

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
			x30 ? set_page_extent_mapped+0x20/0xb0 relocate_file_extent_cluster+0x1a7/0x940 relocate_data_extent+0xaf/0x120 relocate_block_group+0x20f/0x480 btrfs_relocate_block_group+0x152/0x320 btrfs_relocate_chunk+0x3d/0x120 btrfs_reclaim_bgs_work+0x2ae/0x4e0 process_scheduled_works+0x184/0x370 worker_thread+0xc6/0x3e0 ? blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork+0x2f/0x40 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork_asm+0x11/0x20 </TASK> This occurs because cleanup_one_transaction() calls destroy_delalloc_inodes() which calls invalidate_inode_pages2() which takes the folio_lock before setting mapping to NULL. We fail to check		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this, and subsequently call set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode) Note that the "fixes" patch here is not the one that introduced the race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice. **CVE ID: CVE-2024-56758**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.12.8					
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Clear WFE in missing-ENDBRANCH #CPs An indirect branch instruction sets the CPU indirect branch tracker (IBT) into WAIT_FOR_ENDBRANCH (WFE) state and WFE stays asserted across the instruction boundary. When the decoder finds an inappropriate instruction while WFE is set ENDBR, the CPU raises a #CP fault. For the "kernel IBT no ENDBR" selftest where #CPs are deliberately triggered, the WFE state of the interrupted context needs to be cleared to let execution continue. Otherwise when the CPU resumes from the instruction that just caused the previous	https://git.kernel.org/stable/c/b939f108e86b76119428a6fa4e92491e09ac7867, https://git.kernel.org/stable/c/dc81e556f2a017d681251ace21bf06c126d5a192	O-LIN-LINU-200125/1008

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			#CP, another missing-ENDBRANCH #CP is raised and the CPU enters a dead loop. This is not a problem with IDT because it doesn't preserve WFE and IRET doesn't set WFE. But FRED provides space on the entry stack (in an expanded CS area) to save and restore the WFE state, thus the WFE state is no longer clobbered, so software must clear it. Clear WFE to avoid dead looping in ibt_clear_fred_wfe() and the !ibt_fatal code path when execution is allowed to continue. Clobbering WFE in any other circumstance is a security-relevant bug. [dhansen: changelog rewording] **CVE ID: CVE-2024-56761**		
Affected Version(s): From (including) 6.6.53 Up to (excluding) 6.6.66					
Reachable Assertion	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is	https://git.kernel.org/stable/c/2f9bec0a749eb646b384fde0c7b7c24687b2ffae, https://git.kernel.org/stable/c/7064a6daa4a700a298fe3aee11dea296bfe59fc4, https://git.kernel.org/stable/c/b7529880cb961d515642ce63f9d7570869bbbdc3	O-LIN-LINU-200125/1009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reachable from userspace. **CVE ID: CVE-2024-56783**		
Affected Version(s): From (including) 6.6.64 Up to (excluding) 6.6.69					
Double Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free. **CVE ID: CVE-2024-56766**	https://git.kernel.org/stable/c/6ea15205d7e2b811fbbdf79783f686f58abfb4b7, https://git.kernel.org/stable/c/d2f090ea57f8d6587e09d4066f740a8617767b3d, https://git.kernel.org/stable/c/d8e4771f99c0400a1873235704b28bb803c83d17	O-LIN-LINU-200125/1010
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.4					
Use After Free	08-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: kunit: string-stream: Fix a UAF bug in kunit_init_suite() In kunit_debugfs_create_suite(), if alloc_string_stream() fails in the kunit_suite_for_each_test_case() loop, the "suite->log = stream" has assigned before, and the error path only free the suite->log's stream memory but not set it to NULL, so the later string_stream_clear() of suite->log in kunit_init_suite() will cause below UAF bug. Set stream pointer to NULL after free to fix it.	https://git.kernel.org/stable/c/3213b92754b94dec6836e8b4d6ec7d224a805b61, https://git.kernel.org/stable/c/39e21403c978862846fa68b7f6d06f9cca235194	O-LIN-LINU-200125/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Unable to handle kernel paging request at virtual address 006440150000030d Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [006440150000030d] address between user and kernel address ranges Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Dumping ftrace buffer: (ftrace buffer empty) Modules linked in: iio_test_gts industrialio_gts_helper cfg80211 rfkill ipv6 [last unloaded: iio_test_gts] CPU: 5 UID: 0 PID: 6253 Comm: modprobe Tainted: G B W N 6.12.0-rc4+ #458 Tainted: [B]=BAD_PAGE, [W]=WARN, [N]=TEST Hardware name: linux,dummy-virt (DT) pstate: 40000005 (nZcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : string_stream_clear+0x54/0x1ac		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lr : string_stream_clear+0x1a8/0x1ac sp : ffffffc080b47410 x29: ffffffc080b47410 x28: 0064405500000030d x27: ffffff80c96b5e98 x26: ffffff80c96b5e80 x25: fffffffe461b3f6c0 x24: 0000000000000003 x23: ffffff80c96b5e88 x22: 1ffffff019cdf4fc x21: dfffffc000000000 x20: ffffff80ce6fa7e0 x19: 032202a80000186d x18: 0000000000001840 x17: 0000000000000000 x16: 0000000000000000 x15: fffffffe45c355cb4 x14: fffffffe45c35589c x13: fffffffe45c03da78 x12: ffffffb810168e75 x11: 1ffffff810168e74 x10: ffffffb810168e74 x9 : dfffffc000000000 x8 : 0000000000000004 x7 : 0000000000000003 x6 : 0000000000000001 x5 : ffffffc080b473a0 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000001 x1 : fffffffe462fbf620 x0 : dfffffc000000000 Call trace: string_stream_clear+0x54/0x1ac __kunit_test_suites_init+0x108/0x1d8		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kunit_exec_run_tests+0xb8/0x100 kunit_module_notify+0x400/0x55c notifier_call_chain+0xfc/0x3b4 blocking_notifier_call_chain+0x68/0x9c do_init_module+0x24c/0x5c8 load_module+0x4acc/0x4e90 init_module_from_file+0xd4/0x128 idempotent_init_module+0x2d4/0x57c __arm64_sys_finit_module+0xac/0x100 invoke_syscall+0x6c/0x258 el0_svc_common.constprop.0+0x160/0x22c do_el0_svc+0x44/0x5c el0_svc+0x48/0xb8 el0t_64_sync_handler+0x13c/0x158 el0t_64_sync+0x190/0x194 Code: f9400753 d2dff800 f2fbffe0 d343fe7c (38e06b80) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception **CVE ID: CVE-2024-56772**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the	https://git.kern	O-LIN-LINU-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			following vulnerability has been resolved: mtd: spinand: winbond: Fix 512GW, 01GW, 01JW and 02JW ECC information These four chips: * W25N512GW * W25N01GW * W25N01JW * W25N02JW all require a single bit of ECC strength and thus feature an on-die Hamming-like ECC engine. There is no point in filling a ->get_status() callback for them because the main ECC status bytes are located in standard places, and retrieving the number of bitflips in case of corrected chunk is both useless and unsupported (if there are bitflips, then there is 1 at most, so no need to query the chip for that). Without this change, a kernel warning triggers every time a bit flips. **CVE ID: CVE-2024-56771**	el.org/stable/c/234d5f75c3ae911b52c5e4442b8a87fbbd129836, https://git.kernel.org/stable/c/fee9b240916df82a8b07aef0fdfe96785417a164	200125/1012
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent	https://git.kernel.org/stable/c/3ed51857a50f530ac7a1482e069dfbd1298558d4, https://git.kernel.org/stable/c/757171d1369b3b47f36932d40a05a0715496dcab, https://git.kernel.org/stable/c/93992c3d9629b	O-LIN-LINU-200125/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot(). **CVE ID: CVE-2024-56774**	02dccf6849238559d5c24f2dece	
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56777**	https://git.kernel.org/stable/c/3cf2e7c448e246f7e700c7aa47450d1e27579559, https://git.kernel.org/stable/c/997b64c3f4c1827c5cfda8ae7f5d13f78d28b541, https://git.kernel.org/stable/c/b79612ed6bc1a184c45427105c851b5b2d4342ca	O-LIN-LINU-200125/1014
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56776**	https://git.kernel.org/stable/c/40725c5fabee804fecce41d4d5c5bae80c45e1c4, https://git.kernel.org/stable/c/831214f77037de02afc287eae93ce97f218d8c04, https://git.kernel.org/stable/c/8ab73ac97c0fa528f66eeccd9bb53eb6eb7d20dc	O-LIN-LINU-200125/1015

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 Release of Memory after Effective Lifetime	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur The action force umount(umount -f) will attempt to kill all rpc_task even umount operation may ultimately fail if some files remain open. Consequently, if an action attempts to open a file, it can potentially send two rpc_task to nfs server. NFS CLIENT thread1 thread2 open("file") ... nfs4_do_open _nfs4_do_open _nfs4_open_and_get_state _nfs4_proc_open nfs4_run_open_task /* rpc_task1 */ rpc_run_task rpc_wait_for_completion_task umount -f nfs_umount_begin rpc_killall_tasks rpc_signal_task rpc_task1 been wakeup and return -512 _nfs4_do_open // while loop ... nfs4_run_open_task /* rpc_task2 */	https://git.kernel.org/stable/c/0ab0a3ad24e970e894abcac58f85c332d1726749, https://git.kernel.org/stable/c/2d505a801e57428057563762f67a5a62009b2600, https://git.kernel.org/stable/c/37dfc81266d3a32294524bfadd3396614f8633ee	O-LIN-LINU-200125/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			rpc_run_task
			
			rpc_wait_for_completion_task
			
			While processing an open request, nfsd will first attempt to find or allocate an nfs4_openowner. If it finds an nfs4_openowner that is not marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since two rpc_task can attempt to open the same file simultaneously from the client to server, and because two instances of nfsd can run concurrently, this situation can lead to lots of memory leak.
			Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be triggered.
			
			NFS SERVER
			nfsd1 nfsd2
			echo 0 > /proc/fs/nfsd/threads
			
			nfsd4_open
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// alloc oo1, stateid1
			nfsd4_open
			
			nfsd4_process_open1
			
			find_or_alloc_open_stateowner
			// find oo1, without NFS4_OO_CONFIRMED
			
			release_openowner		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			unhash_openowner_locked
			
			list_del_init(&oo->oo_perclient)
			// cannot find this oo
			// from client, LEAK!!!
			
			alloc_stateowner // alloc oo2
			
			nfsd4_process_open2
			init_open_stateid
			// associate oo1
			// with stateid1, stateid1 LEAK!!!
			nfs4_get_vfs_file
			// alloc nfsd_file1 and nfsd_file_mark1
			// all LEAK!!!
			
			nfsd4_process_open2
			...
			
			write_threads
			...
			
			nfsd_destroy_serv
			
			nfsd_shutdown_net
			
			nfs4_state_shutdown_net
			
			nfs4_state_destroy_net
			
			destroy_client
			
			__destroy_client
			// won't find oo1!!!
			
			nfsd_shutdown_generic
			
			nfsd_file_cache_shutdown
			
			kmem_cache_destroy for nfsd_file_slab		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 nfsd_file_mark_slab // bark since nfsd_file1 // and nfsd_file_mark1 // still alive ========== ========== ========== ======== BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on __kmem_cache_shutdown() ---------- ---------- Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28 flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff) CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.1-2.fc37 04/01/2014 Call Trace: <TASK> dum ---truncated--- **CVE ID: CVE-2024-56779**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super()	https://git.kernel.org/stable/c/3e6ff207cd5bd924ad94cd1a7c633bcdac0ba1cb, https://git.kernel.org/stable/c/6f3821acd7c314314599924808 7de5fb4b48cf26 , https://git.kern	O-LIN-LINU-200125/1017

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores.	el.org/stable/c/8ea87e34792258825d290f4dc5216276e91cb224	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze. **CVE ID: CVE-2024-56780**		
Improper Check for Unusual or Exceptional Conditions	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure. **CVE ID: CVE-2024-56778**	https://git.kernel.org/stable/c/31c857e7496d34e5a32a6f75bc024d0b06fd646a, https://git.kernel.org/stable/c/6b0d0d6e9d3c26697230bf7dc9e6b52bdb24086f, https://git.kernel.org/stable/c/82a5312f874fb18f045d9658e9bd290e3b0621c0	O-LIN-LINU-200125/1018
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.5					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-	https://git.kernel.org/stable/c/0b94d838018fb0a824e0cd3149034928c99fb1b7, https://git.kernel.org/stable/c/296a109fa77110ba5267fe0e90a26005eecc2726, https://git.kernel.org/stable/c/691284c2cd33ffaa0b35ce53b3286b90621e9dc9	O-LIN-LINU-200125/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108 Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-56781		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: bpf: put bpf_link's program when link is safe to be deallocated In general, BPF link's underlying BPF program should be considered to be reachable through attach hook -> link -> prog chain, and, pessimistically, we have to assume that as long as link's memory is not safe to free, attach hook's code might hold a pointer to BPF program and use it. As such, it's not (generally) correct to put link's program early before waiting for RCU GPs to go through. More eager bpf_prog_put() that we currently do is mostly correct due to BPF program's release code doing similar RCU GP waiting, but as will be shown in the following patches, BPF program can be non-sleepable (and, thus, reliant on only "classic" RCU GP), while BPF link's attach hook can have sleepable semantics and needs to be protected by RCU Tasks Trace, and for such cases BPF link has to go through RCU Tasks Trace + "classic" RCU GPs before being deallocated. And so, if we put BPF program early, we might free BPF	https://git.kernel.org/stable/c/2fcb921c2799c49ac5e365cf4110f94a64ae4885, https://git.kernel.org/stable/c/5fe23c57abadfd46a7a66e81f3536e4757252a0b, https://git.kernel.org/stable/c/f44ec8733a8469143fde1984b5e6931b2e2f6f3f	O-LIN-LINU-200125/1020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			program before we free BPF link, leading to use-after-free situation. So, this patch defers bpf_prog_put() until we are ready to perform bpf_link's deallocation. At worst, this delays BPF program freeing by one extra RCU GP, but that seems completely acceptable. Alternatively, we'd need more elaborate ways to determine BPF hook, BPF link, and BPF program lifetimes, and how they relate to each other, which seems like an unnecessary complication. Note, for most BPF links we still will perform eager bpf_prog_put() and link dealloc, so for those BPF links there are no observable changes whatsoever. Only BPF links that use deferred dealloc might notice slightly delayed freeing of BPF programs. Also, to reduce code and logic duplication, extract program put + link dealloc logic into bpf_link_dealloc() helper. **CVE ID: CVE-2024-56786**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is	https://git.kernel.org/stable/c/2129f6faa5dfe8c6b87aad11720bf75edd77d3e4, https://git.kernel.org/stable/c/997a3c04d7fa3d1d385c14691350d096fada648	O-LIN-LINU-200125/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns -EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. " ----------[cut here]---------- WARNING: CPU: 1 PID: 1 at drivers/soc/imx/soc-imx8m.c:115 imx8mm_soc_revision+0xdc/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924-00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--)	c, https://git.kernel.org/stable/c/9cc832d37799dbea950c4c8a34721b02b8b5a8ff	

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pc : imx8mm_soc_revision+0xdc /0x180 lr : imx8mm_soc_revision+0xd 0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbce0 x28: 0000000000000000 x27: ffff800081810120 x26: ffff8000818a9970 x25: 0000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffdfb x20: ffff800082780000 x19: 0000000000000001 x18: ffffffffffffffff x17: ffff800081fff418 x16: ffff8000823e1000 x15: ffff0000c03b65e8 x14: ffff0000c00051b0 x13: ffff800082790000 x12: 0000000000000801 x11: ffff80008278ffff x10: ffff80008209d3a6 x9 : ffff80008062e95c x8 : ffff8000821fb9a0 x7 : 0000000000000000 x6 : 00000000000080e3 x5 : ffff0000df8c03d8 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1 : fffffffffffffdfb x0 : fffffffffffffdfb Call trace: imx8mm_soc_revision+0xdc /0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a 8 kernel_init_freeable+0x240 /0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20 ---[end trace 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
			SoC: i.MX8MP revision 1.1 " **CVE ID: CVE-2024-56787**		
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0	https://git.kernel.org/stable/c/01575f2ff8ba578a3436f230668bd056dc2eb823, https://git.kernel.org/stable/c/4fbd66d8254cedfd1218393f39d83b6c07a01917, https://git.kernel.org/stable/c/5a2eaa3ad2b803c7ea442c6db7379466ee73c024	O-LIN-LINU-200125/1022

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a). **CVE ID: CVE-2024-56785**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.6					
N/A	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: net/sched: netem: account for backlog updates from child qdisc In general, 'qlen' of any classful qdisc should keep track of the number of packets that the qdisc itself and all of its children holds. In case of netem, 'qlen' only accounts for the packets in its internal tfifo. When netem is used with a child qdisc, the child qdisc can use 'qdisc_tree_reduce_backlog' to inform its parent, netem, about created or dropped SKBs. This function updates 'qlen' and the backlog statistics of netem, but netem does not account for changes made by a child qdisc. 'qlen' then indicates the wrong number of packets in the tfifo. If a child qdisc creates new SKBs during enqueue and informs its parent about this, netem's 'qlen'	https://git.kernel.org/stable/c/10df49cfca73dfbbdb6c4150d859f7e8926ae427, https://git.kernel.org/stable/c/216509dda290f6db92c816dd54b83c1df9da9e76, https://git.kernel.org/stable/c/356078a5c55ec8d2061fcc009fb8599f5b0527f9	O-LIN-LINU-200125/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			value is increased. When netem dequeues the newly created SKBs from the child, the 'qlen' in netem is not updated. If 'qlen' reaches the configured sch->limit, the enqueue function stops working, even though the tfifo is not full.
			
			Reproduce the bug: Ensure that the sender machine has GSO enabled. Configure netem as root qdisc and tbf as its child on the outgoing interface of the machine
			as follows:
			$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
			$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
			
			Send bulk TCP traffic out via this interface, e.g., by running an iPerf3 client on the machine. Check the qdisc statistics:
			$ tc -s qdisc show dev <oif>
			
			Statistics after 10s of iPerf3 TCP test before the fix (note that
			netem's backlog > limit, netem stopped accepting packets):
			qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0)
			backlog 4294528236b 1155p requeues 0
			qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms
			Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem'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
			backlog statistics. **CVE ID: CVE-2024-56770**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.8					
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX	https://git.kernel.org/stable/c/05aa156e156ef3168e7ab8a68721945196495c17, https://git.kernel.org/stable/c/6d9cd27105459f169993a4c5f216499a946dbf34, https://git.kernel.org/stable/c/8b2282b5084521254a2cd9742a3f4e1d5b77f843	O-LIN-LINU-200125/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c0000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c0000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c0000000006eb5c8] __asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c00000000013f898] reconfig_close_windows+0x1a0/0x4e8 [16386.255343] [c00000016b297990] [c000000000140e58] vas_migration_handler+0x3a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0x4c/0x4c4 ... [16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x68 [16386.256163] kasan_save_track+0x34/0x80 [16386.256175] kasan_save_alloc_info+0x58/0x74		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[16386.256196] __kasan_slab_alloc+0xb8/0xdc [16386.256209] kmem_cache_alloc_noprof+0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x24c [16386.256292] ksys_mmap_pgoff+0x20c/0x348 [16386.256303] sys_mmap+0xd0/0x160 ... [16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x68 [16386.256374] kasan_save_track+0x34/0x80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396] __kasan_slab_free+0x120/0x204 [16386.256415] kmem_cache_free+0x128/0x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x60c [16386.256495]		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_softirq_own_stack+0x6c /0x88 [16386.256509] do_softirq_own_stack+0x58 /0x88 [16386.256521] __irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepar e.constprop.0+0x18/0x2c ... [16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x 68 [16386.256741] __kasan_record_aux_stack+0 xcc/0x12c [16386.256753] __call_rcu_common.constpro p.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.cons tprop.0+0x684/0x870 [16386.256811] __vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a 0/0x4a0 [16386.256841] system_call_vectored_comm on+0x15c/0x2ec [16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy		

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14a81 [16386.256950] memcg:c0000000ba430001 [16386.256961] anon flags: 0x43ffff800000000(node=4|zone=0|lastcpupid=0x7ffff) [16386.256975] page_type: 0xfdffffff(slab) [16386 ---truncated--- **CVE ID: CVE-2024-56765**		
Use After Free	06-Jan-2025	7.8	In the Linux kernel, the following vulnerability has been resolved: ublk: detach gendisk from ublk device if add_disk() fails Inside ublk_abort_requests(), gendisk is grabbed for aborting all inflight requests. And ublk_abort_requests() is called when exiting the uring context or handling timeout. If add_disk() fails, the gendisk may have been freed when calling ublk_abort_requests(), so use-after-free can be caused when getting disk's reference in ublk_abort_requests().	https://git.kernel.org/stable/c/75cd4005da5492129917a4a4ee45e816605561044, https://git.kernel.org/stable/c/7d680f2f76a3417fdfc3946da7471e81464f7b41	O-LIN-LINU-200125/1025

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fixes the bug by detaching gendisk from ublk device if add_disk() fails. **CVE ID: CVE-2024-56764**		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Handle lack of irqdomain gracefully Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2c/0x32 __pci_enable_msix_range+0x30c/0x596 pci_msi_setup_msi_irqs+0x2c/0x32 pci_alloc_irq_vectors_affinity+0xb8/0xe2 RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub. That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy	https://git.kernel.org/stable/c/a60b990798eb17433d0283788280422b1bd94b18, https://git.kernel.org/stable/c/aed157301c659a48f5564cc4568cf0e5c8831af0, https://git.kernel.org/stable/c/b1f7476e07b93d65a1a3643dcb4a7bed80d4328d	O-LIN-LINU-200125/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP. Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are weak implementations which return an error, so the problem was papered over. Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it. **CVE ID: CVE-2024-56760**		
N/A	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it. **CVE ID: CVE-2024-56763**	https://git.kernel.org/stable/c/03041e474a6a8f1bfd4b96b164bb3165c48fa1a3, https://git.kernel.org/stable/c/1cca920af19df5dd91254e5ff35e68e911683706, https://git.kernel.org/stable/c/3d15f4c2449558ffe83b4dba30614ef1cd6937c3	O-LIN-LINU-200125/1027
Use of Uninitialized Resource	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue	https://git.kernel.org/stable/c/1d6de21f00293d819b5ca6dbe75ff1f3b6392140, https://git.kernel.org/stable/c/2dd59fe0e19e1ab9552599780882b62e5751924c	O-LIN-LINU-200125/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values. Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem. [1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ========== ========== ========== BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dibusb_dib3000mb_frontend_attach+0x155/0x2f0 drivers/media/usb/dvb-usb/dibusb-mb.c:31 dvb_usb_adapter_frontend_init+0xed/0x9a0 drivers/media/usb/dvb-usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:186 [inline]	7, https://git.kernel.org/stable/c/3876e3a1c31a58a352c6bf5d2a90e3304445a637	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			dvb_usb_device_init+0x25a8/0x3760 drivers/media/usb/dvb-usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb-usb/dibusb-mb.c:110 ... Local variable rb created at: dib3000_read_reg+0x86/0x4e0 drivers/media/dvb-frontends/dib3000mb.c:54 dib3000mb_attach+0x123/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 ... **CVE ID: CVE-2024-56769**		
NULL Pointer Dereference	06-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memset The at_xdmac_memset_create_desc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this. **CVE ID: CVE-2024-56767**	https://git.kernel.org/stable/c/54376d8d26596f98ed7432a788314bb9154bf3e3, https://git.kernel.org/stable/c/c43ec96e8d34399bd9dab2f2dc316b9048921333f, https://git.kernel.org/stable/c/e658f1c133b854b2ae799147301d82dddb8f3162	O-LIN-LINU-200125/1029
Affected Version(s): From (including) 6.8 Up to (excluding) 6.12.4					
NULL Pointer Dereference	08-Jan-2025	5.5	In the Linux kernel, the following vulnerability has been resolved: kunit: Fix potential null dereference in kunit_device_driver_test()	https://git.kernel.org/stable/c/435c20eed572a95709b1536ff78832836b2f91b1, https://git.kern	O-LIN-LINU-200125/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kunit_kzalloc() may return a NULL pointer, dereferencing it without NULL check may lead to NULL dereference. Add a NULL check for test_state. **CVE ID: CVE-2024-56773**	el.org/stable/c/5d28fac59369b5d3c48cdf09e50275a61ff91202	
Vendor: Microsoft					
Product: windows_10_21h2					
Affected Version(s): * Up to (excluding) 10.0.19044.5371					
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1031
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21334**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334	O-MIC-WIND-200125/1032
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1033
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.5371					
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1034
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1035
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege	https://msrc.microsoft.com/update-	O-MIC-WIND-200125/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability **CVE ID: CVE-2025-21334**	guide/vulnerability/CVE-2025-21334	
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4751					
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1037
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21334**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334	O-MIC-WIND-200125/1038
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1039
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4751					
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1040
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1041
Affected Version(s): * Up to (excluding) 10.0.22631.4751					
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1042
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability	https://msrc.microsoft.com/update-guide/vulnerabi	O-MIC-WIND-200125/1043

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2025-21334	lity/CVE-2025-21334	
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1044
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.2894					
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1045
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1046
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21334**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334	O-MIC-WIND-200125/1047
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1369					
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1048
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21334**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334	O-MIC-WIND-200125/1049
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1050

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_2025					
Affected Version(s): * Up to (excluding) 10.0.26100.2894					
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21334**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334	O-MIC-WIND-200125/1051
Use After Free	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21335**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335	O-MIC-WIND-200125/1052
Heap-based Buffer Overflow	14-Jan-2025	7.8	Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21333**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333	O-MIC-WIND-200125/1053
Vendor: Qualcomm					
Product: aqt1000_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-AQT1-200125/1054
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-AQT1-200125/1055
Product: ar8035_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-AR80-200125/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-AR80-200125/1057
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-AR80-200125/1058
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-C-V2-200125/1059
Product: csr8811_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-CSR8-200125/1060
Product: csrb31024_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-CSRB-200125/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: fastconnect_6200_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1062
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1063
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1064
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1065
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1066
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qualcomm.com/product/publicresources/security	O-QUA-FAST-200125/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin/january-2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1068
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1069
Product: fastconnect_6800_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1070
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1071
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1072
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Buffer Copy	06-Jan-2025	8.4	Memory corruption while	https://docs.qu	O-QUA-FAST-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1073
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1074
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1076
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1077
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1078
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-FAST-200125/1079

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45550	bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1080
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1081
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1082
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1083
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1084
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1085
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Buffer Copy	06-Jan-2025	8.4	Memory corruption while	https://docs.qu	O-QUA-FAST-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1086
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1087
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1089
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1090
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1091
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-FAST-200125/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1093
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1094
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1095
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1096
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1097
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-FAST-200125/1098
Product: flight_rb5_5g_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	O-QUA-FLIG-200125/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: immersive_home_214_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IMME-200125/1100
Product: immersive_home_216_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IMME-200125/1101
Product: immersive_home_316_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IMME-200125/1102
Product: immersive_home_318_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-IMME-200125/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Product: immersive_home_3210_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IMME-200125/1104
Product: immersive_home_326_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IMME-200125/1105
Product: ipq5010_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1106
Product: ipq5028_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1107
Product: ipq5300_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1108
Product: ipq5302_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1109
Product: ipq5312_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1110
Product: ipq5332_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ5-200125/1111
Product: ipq6000_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-IPQ6-200125/1112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: ipq6010_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ6-200125/1113
Product: ipq6018_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ6-200125/1114
Product: ipq6028_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ6-200125/1115
Product: ipq8070a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1116
Product: ipq8071a_firmware					
Affected Version(s): -					
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-IPQ8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1117
Product: ipq8072a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1118
Product: ipq8074a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1119
Product: ipq8076a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1120
Product: ipq8076_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: ipq8078a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1122
Product: ipq8078_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1123
Product: ipq8173_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1124
Product: ipq8174_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ8-200125/1125
Product: ipq9008_firmware					
Affected Version(s): -					
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-IPQ9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1126
Product: ipq9048_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ9-200125/1127
Product: ipq9554_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ9-200125/1128
Product: ipq9570_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ9-200125/1129
Product: ipq9574_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-IPQ9-200125/1130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: msm8996au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-MSM8-200125/1131
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-MSM8-200125/1132
Product: qam8255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1133
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1134

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1135
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1136
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1137
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1138
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1139
Product: qam8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1140

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45555		
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1141
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1142
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1143
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1144
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1145
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1146
Buffer Over-	06-Jan-2025	6.1	Information disclosure	https://docs.qu	O-QUA-QAM8-

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1147
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1148
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1149
Product: qam8620p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1150
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1151
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QAM8-200125/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global registers through SMMU. **CVE ID: CVE-2024-43064**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1153
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1154
Product: qam8650p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1155
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1156
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QAM8-200125/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1158
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1159
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1160
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1161
Product: qam8775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1162
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QAM8-200125/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1164
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1165
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1166
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1167
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAM8-200125/1168
Product: qamsrv1h_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QAMS-200125/1169

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1170
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1171
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1172
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1173
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1174
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-	https://docs.qualcomm.com/product/publicres	O-QUA-QAMS-200125/1175

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FastRPC backend. **CVE ID: CVE-2024-45559**	ources/security bulletin/january -2025-bulletin.html	
Product: qamsrv1m_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1176
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1177
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1178
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QAMS-200125/1179
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QAMS-200125/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45559	-2025-bulletin.html	
Product: qca0000_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA0-200125/1181
Product: qca1062_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA1-200125/1182
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA1-200125/1183
Product: qca1064_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA1-200125/1184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA1-200125/1185
Product: qca2062_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1186
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1187
Product: qca2064_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1188
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1189
Product: qca2065_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1190
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1191
Product: qca2066_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1192
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA2-200125/1193
Product: qca4024_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA4-200125/1194
Product: qca6174a_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1195
Product: qca6310_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1196

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qca6320_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1197
Product: qca6391_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1198
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1199
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1200
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1201
Product: qca6420_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
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1203
Product: qca6426_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1204
Product: qca6430_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1205
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1206
Product: qca6436_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCA6-200125/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33067	bulletin.html	
Product: qca6554a_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1208
Product: qca6564au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1209
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1210
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1211
Product: qca6564a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-200125/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1213
Product: qca6574au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1214
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1215
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1217
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1218
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1219
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1220
Product: qca6574a_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1221
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCA6-200125/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1223
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1224
Product: qca6574_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1225
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1226
Product: qca6584au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-200125/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1228
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1229
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1230
Product: qca6595au_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1231
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-QCA6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1232
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1233
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1234
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1235
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1236
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1237
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCA6-200125/1238

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1239
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1240
Product: qca6595_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1241
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1242
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1243

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
			CVE ID: CVE-2024-43064		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1244
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1245
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1246
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1247
Product: qca6678aq_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1248
Product: qca6688aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCA6-200125/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1250
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1251
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1252
Product: qca6696_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1253
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	O-QUA-QCA6-200125/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1255
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1256
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1257
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1258
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1259
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCA6-200125/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1261
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1262
Product: qca6698aq_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1263
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1264
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1265
N/A	06-Jan-2025	7.5	Uncontrolled resource	https://docs.qu	O-QUA-QCA6-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1266
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1267
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1268
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1269
Product: qca6777aq_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1270
Product: qca6787aq_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558		
Product: qca6797aq_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1272
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA6-200125/1273
Product: qca8075_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1274
Product: qca8081_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1275
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-QCA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1276
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1277
Product: qca8082_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1278
Product: qca8084_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1279
Product: qca8085_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1280
Product: qca8337_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1281
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1282
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1283
Product: qca8386_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA8-200125/1284
Product: qca9367_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA9-200125/1285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca9377_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA9-200125/1286
Product: qca9888_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA9-200125/1287
Product: qca9889_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCA9-200125/1288
Product: qcc2073_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1289
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCC2-200125/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1291
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1292
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1293
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1294
Product: qcc2076_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1295
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1296
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-QCC2-200125/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45548	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1299
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC2-200125/1300
Product: qcc710_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC7-200125/1301
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCC7-200125/1302
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model	https://docs.qualcomm.com/product/publicres	O-QUA-QCC7-200125/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	ources/security bulletin/january -2025-bulletin.html	
Product: qcf8000sfp_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCF8-200125/1304
Product: qcf8000_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCF8-200125/1305
Product: qcf8001_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCF8-200125/1306
Product: qcm4325_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM4-200125/1307

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Product: qcm4490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM4-200125/1308
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM4-200125/1309
Product: qcm5430_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM5-200125/1310
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM5-200125/1311
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM5-200125/1312
Product: qcm6490_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): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM6-200125/1313
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM6-200125/1314
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM6-200125/1315
Product: qcm8550_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM8-200125/1316
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM8-200125/1317
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCM8-200125/1318
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to	https://docs.qualcomm.com/pr	O-QUA-QCM8-200125/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unmap the DMA buffers. **CVE ID: CVE-2024-33055**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: qcn5022_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1320
Product: qcn5024_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1321
Product: qcn5052_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1322
Product: qcn5122_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1323
Product: qcn5124_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): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1324
Product: qcn5152_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1325
Product: qcn5154_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1326
Product: qcn5164_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN5-200125/1327
Product: qcn6023_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QCN6-200125/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Product: qcn6024_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1329
Product: qcn6112_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1330
Product: qcn6122_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1331
Product: qcn6132_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1332
Product: qcn6224_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1333
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1334
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1335
Product: qcn6274_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1336
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1337
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback	https://docs.qualcomm.com/pr	O-QUA-QCN6-200125/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: qcn6402_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1339
Product: qcn6412_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1340
Product: qcn6422_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1341
Product: qcn6432_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN6-200125/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn7605_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN7-200125/1343
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN7-200125/1344
Product: qcn7606_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN7-200125/1345
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN7-200125/1346
Product: qcn9000_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1347
Product: qcn9012_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	O-QUA-QCN9-200125/1348

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
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Product: qcn9022_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1349
Product: qcn9024_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1350
Product: qcn9070_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1351
Product: qcn9072_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn9074_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1353
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1354
Product: qcn9100_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1355
Product: qcn9160_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCN9-200125/1356
Product: qcn9274_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QCN9-200125/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Product: qcs410_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS4-200125/1358
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS4-200125/1359
Product: qcs4490_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS4-200125/1360
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS4-200125/1361
Product: qcs5430_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QCS5-200125/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-45541**	-2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS5-200125/1363
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS5-200125/1364
Product: qcs610_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1365
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1366
Product: qcs6490_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1367
Buffer Copy without Checking Size of Input ('Classic	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QCS6-200125/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			**CVE ID: CVE-2024-45541**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1369
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1370
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS6-200125/1371
Product: qcs7230_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS7-200125/1372
Product: qcs8250_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1373

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-2024-45553		
Product: qcs8550_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1374
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1375
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1376
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1377
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS8-200125/1378
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-QCS8-200125/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33041	-2025-bulletin.html	
Product: qcs9100_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QCS9-200125/1380
Product: qdu1000_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QDU1-200125/1381
Product: qdu1010_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QDU1-200125/1382
Product: qdu1110_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-QDU1-200125/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Product: qdu1210_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QDU1-200125/1384
Product: qdx1010_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QDX1-200125/1385
Product: qdx1011_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QDX1-200125/1386
Product: qep8111_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QEP8-200125/1387
Product: qfw7114_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1388
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1389
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1390
Product: qfw7124_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1392
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QFW7-200125/1393
Product: qrb5165n_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QRB5-200125/1394
Product: qru1032_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QRU1-200125/1395
Product: qru1052_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QRU1-200125/1396
Product: qru1062_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QRU1-200125/1397
Product: qsm8250_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QSM8-200125/1398
Product: qxm8083_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-QXM8-200125/1399
Product: robotics_rb5_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-ROBO-200125/1400
Product: sa6145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1401
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1402
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1403
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1404
Product: sa6150p_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): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1405
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1406
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1407
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1408
Product: sa6155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1409

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1410
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1411
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1412
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1413
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1414
Product: sa6155_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images,	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA61-200125/1415

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**		
Product: sa7255p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA72-200125/1416
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA72-200125/1417
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA72-200125/1418
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA72-200125/1419
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA72-200125/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45559	bulletin/january-2025-bulletin.html	
Product: sa7775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA77-200125/1421
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA77-200125/1422
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA77-200125/1423
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA77-200125/1424
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SA77-200125/1425

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sa8145p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1426
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1427
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1428
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1429
Product: sa8150p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1430

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45555		
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1431
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1432
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1433
Product: sa8155p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1434
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1435
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-SA81-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1436
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1437
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1438
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1439
Product: sa8155_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1440
Product: sa8195p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA81-200125/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1442
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1443
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1444
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1445
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA81-200125/1446
Product: sa8255p_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): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1447
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1448
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1449
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1450
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1451
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API.	https://docs.qualcomm.com/product/publicres	O-QUA-SA82-200125/1452

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43063	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1453
Product: sa8295p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1454
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1455
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1456
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SA82-200125/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45558	bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1458
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1459
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1460
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1461
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1462
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA82-200125/1463
Product: sa8530p_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	O-QUA-SA85-200125/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1465
Product: sa8540p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1466
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1467
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1468
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1469

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1470
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1471
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA85-200125/1472
Product: sa8620p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1473
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1474
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU	https://docs.qualcomm.com/product/publicres	O-QUA-SA86-200125/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1476
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1477
Product: sa8650p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1478
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1479
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-SA86-200125/1480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1481
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1482
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1483
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA86-200125/1484
Product: sa8770p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1485
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA87-200125/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin/january-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1487
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1488
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1489
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1490
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1491
Product: sa8775p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA87-200125/1492

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1493
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1494
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1495
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1496
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA87-200125/1497
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific	https://docs.qualcomm.com/pr	O-QUA-SA87-200125/1498

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: sa9000p_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1499
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1500
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1501
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1502
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SA90-200125/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than mailbox size. **CVE ID: CVE-2024-23366**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1504
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1505
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SA90-200125/1506
Product: sc8180x-aaab_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1507
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1508
Product: sc8180x-acaf_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SC81-200125/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1510
Product: sc8180x-ad_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1511
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1512
Product: sc8180xp-aaab_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1513
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1514
Product: sc8180xp-acaf_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SC81-200125/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1516
Product: sc8180xp-ad_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1517
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1518
Product: sc8180x\+sdx55_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC81-200125/1520
Product: sc8280xp-abbb_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SC82-200125/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC82-200125/1522
Product: sc8380xp_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC83-200125/1523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC83-200125/1524
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC83-200125/1525
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC83-200125/1526
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SC83-200125/1527
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-SC83-200125/1528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45548	bulletin/january-2025-bulletin.html	
Product: sd835_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SD83-200125/1529
Product: sd865_5g_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SD86-200125/1530
Product: sdm429w_firmware					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SDM4-200125/1531
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SDM4-200125/1532
Product: sdx55_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries	https://docs.qualcomm.com/product/publicres	O-QUA-SDX5-200125/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	ources/security bulletin/january -2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SDX5-200125/1534
Product: sdx65m_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SDX6-200125/1535
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SD_8-200125/1536
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SD_8-200125/1537
Product: sg4150p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	O-QUA-SG41-200125/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: sg8275p_firmware					
Affected Version(s): -					
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SG82-200125/1539
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SG82-200125/1540
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SG82-200125/1541
Product: sm4635_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM46-200125/1542
Product: sm6250_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')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM62-200125/1543
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM62-200125/1544
Product: sm6650_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM66-200125/1545
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM66-200125/1546
Product: sm7635_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM76-200125/1547
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-SM76-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1548
Product: sm7675p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM76-200125/1549
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM76-200125/1550
Product: sm7675_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM76-200125/1551
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM76-200125/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: sm8550p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM85-200125/1553
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM85-200125/1554
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM85-200125/1555
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM85-200125/1556
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM85-200125/1557
Product: sm8635p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-SM86-200125/1558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM86-200125/1559
Product: sm8635_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM86-200125/1560
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM86-200125/1561
Product: sm8750p_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM87-200125/1562
Product: sm8750_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	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SM87-200125/1563
Product: snapdragon_429_mobile_firmware					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1564
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1565
Product: snapdragon_460_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1566
Product: snapdragon_480\+_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SNAP-200125/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Product: snapdragon_480_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1568
Product: snapdragon_4_gen_1_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1569
Product: snapdragon_4_gen_2_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1570
Product: snapdragon_662_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1571
Product: snapdragon_680_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1572
Product: snapdragon_685_4g_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1573
Product: snapdragon_695_5g_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1574

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1575
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1576
Product: snapdragon_7c_compute_platform_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1578
Product: snapdragon_7c_gen_2_compute_platform_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1579
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-SNAP-200125/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025-bulletin.html	
Product: snapdragon_820_automotive_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1581
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1582
Product: snapdragon_835_mobile_pc_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1583
Product: snapdragon_865\+_5g_mobile_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1584
Product: snapdragon_865_5g_mobile_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1585
Product: snapdragon_870_5g_mobile_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1586
Product: snapdragon_8\+_gen_1_mobile_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1587
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1588
Product: snapdragon_8\+_gen_2_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arise. **CVE ID: CVE-2024-45553**		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1590
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1591
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1592
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1593
Product: snapdragon_8_gen_1_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1594
Product: snapdragon_8_gen_2_mobile_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	O-QUA-SNAP-200125/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1596
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1597
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1598
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1599
Product: snapdragon_8_gen_3_mobile_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1600
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	O-QUA-SNAP-200125/1601

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1602
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1603
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1604
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1605
Product: snapdragon_ar1_gen_1_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1606

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_ar2_gen_1_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1607
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1608
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1609
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1610
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-SNAP-200125/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1612
Product: snapdragon_w5\+_gen_1_wearable_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1613
Product: snapdragon_x35_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1614
Product: snapdragon_x55_5g_modem-rf_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1615

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_x65_5g_modem-rf_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1616
Product: snapdragon_x72_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1617
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1618
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1619
Product: snapdragon_x75_5g_modem-rf_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-SNAP-200125/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1621
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1622
Product: snapdragon_xr2_5g_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SNAP-200125/1623
Product: srv1h_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1624
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the	https://docs.qualcomm.com/product/publicres	O-QUA-SRV1-200125/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	ources/security bulletin/january-2025-bulletin.html	
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1626
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1627
Buffer Over-read	06-Jan-2025	6.6	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size. **CVE ID: CVE-2024-23366**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1628
Buffer Over-read	06-Jan-2025	6.1	information disclosure while invoking the mailbox read API. **CVE ID: CVE-2024-43063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1629
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1630
Product: srv1l_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten,	https://docs.qualcomm.com/product/publicres	O-QUA-SRV1-200125/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	ources/security bulletin/january -2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1632
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1633
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1634
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1635
Product: srv1m_firmware					
Affected Version(s): -					
Out-of-bounds Write	06-Jan-2025	8.4	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-SRV1-200125/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image. **CVE ID: CVE-2024-45555**	-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1637
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1638
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1639
Buffer Over-read	06-Jan-2025	5.5	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend. **CVE ID: CVE-2024-45559**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SRV1-200125/1640
Product: ssg2115p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specific task, issues may arise. **CVE ID: CVE-2024-45553**		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1642
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1643
Product: ssg2125p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1644
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1645
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SSG2-200125/1646
Product: sw5100p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	O-QUA-SW51-200125/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SW51-200125/1648
Product: sw5100_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SW51-200125/1649
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SW51-200125/1650
Product: sxr1230p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR1-200125/1651

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR1-200125/1652
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR1-200125/1653
Product: sxr2130_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1654
Product: sxr2230p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1655
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1656
Use After	06-Jan-2025	6.7	Memory corruption while	https://docs.qu	O-QUA-SXR2-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1657
Product: sxr2250p_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1658
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1659
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1660
Product: sxr2330p_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-SXR2-200125/1661
Product: talynplus_firmware					
Affected Version(s): -					
Buffer Copy	06-Jan-2025	8.4	Memory corruption while	https://docs.qu	O-QUA-TALY-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1662
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-TALY-200125/1663
Product: video_collaboration_vc1_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1664
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1665
Product: video_collaboration_vc3_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1666
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-VIDE-200125/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-45542	-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1668
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1669
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1670
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1671
Product: video_collaboration_vc5_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-VIDE-200125/1672
Product: wcd9335_firmware					
Affected Version(s): -					
Buffer Over-	06-Jan-2025	6.1	Information disclosure	https://docs.qu	O-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1673
Product: wcd9340_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1674
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1675
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1676
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1677
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9341_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1679
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1680
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1681
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1682
Product: wcd9370_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1683
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1684
Buffer Copy	06-Jan-2025	7.8	Memory corruption when	https://docs.qu	O-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1685
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1686
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1687
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1688
Product: wcd9375_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1690
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1691
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1692
Product: wcd9378_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1693
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1694
Product: wcd9380_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1695
Buffer Copy	06-Jan-2025	7.8	Memory corruption while	https://docs.qu	O-QUA-WCD9-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1696
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1697
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1698
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1699
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1700
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1701
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-WCD9-200125/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			length. **CVE ID: CVE-2024-45558**	-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1703
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1704
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1705
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1706
Product: wcd9385_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1707
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1708
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific	https://docs.qualcomm.com/pr	O-QUA-WCD9-200125/1709

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1711
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1712
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1713
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1714
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	https://docs.qualcomm.com/product/publicresources/securitybulletin/january	O-QUA-WCD9-200125/1715

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33041	-2025-bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1716
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1717
Product: wcd9390_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1718
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1719
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1720
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-	O-QUA-WCD9-200125/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1722
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1723
Product: wcd9395_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1724
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1725
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1726
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1727

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1728
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCD9-200125/1729
Product: wcn3620_firmware					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1730
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1731
Product: wcn3660b_firmware					
Affected Version(s): -					
N/A	06-Jan-2025	7.5	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU. **CVE ID: CVE-2024-43064**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1732
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID: CVE-2024-33061		
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1734
Product: wcn3680b_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1735
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1736
Product: wcn3950_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1737
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1738

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1739
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1740
Product: wcn3980_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1741
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1742
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1743
Product: wcn3988_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN3-200125/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1745
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1746
Product: wcn3990_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN3-200125/1747
Product: wcn6450_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1748
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the	https://docs.qualcomm.com/pr	O-QUA-WCN6-200125/1749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Product: wcn6650_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1750
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1751
Product: wcn6740_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1752
Product: wcn6755_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1753

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-45553		
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN6-200125/1754
Product: wcn7860_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN7-200125/1755
Product: wcn7861_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN7-200125/1756
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN7-200125/1757
Product: wcn7880_firmware					
Affected Version(s): -					
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WCN7-200125/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID without checking the IE length. **CVE ID: CVE-2024-45558**	bulletin/january-2025-bulletin.html	
Product: wcn7881_firmware					
Affected Version(s): -					
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN7-200125/1759
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WCN7-200125/1760
Product: wsa8810_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1761
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1762
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WSA8-200125/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-45541**	bulletin/january-2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1764
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1765
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1766
Product: wsa8815_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1767
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1768
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1769
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1770
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1771
Buffer Over-read	06-Jan-2025	6.1	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver. **CVE ID: CVE-2024-33067**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1772
Product: wsa8830_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1773
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1774
Buffer Copy without Checking Size of Input	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data.	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WSA8-200125/1775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID: CVE-2024-45541**	bulletin/january-2025-bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1776
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1777
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1778
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1779
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1780
Product: wsa8832_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1781
Use After	06-Jan-2025	7.8	Memory corruption can	https://docs.qu	O-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Free			occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1782
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1783
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1784
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1785
Product: wsa8835_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1787
Stack-based Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from	https://docs.qualcomm.com/pr	O-QUA-WSA8-200125/1788

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow			user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1789
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1790
Buffer Over-read	06-Jan-2025	6.8	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process. **CVE ID: CVE-2024-33061**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1791
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1792
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1793
Product: wsa8840_firmware					
Affected Version(s): -					
Buffer Copy without	06-Jan-2025	8.4	Memory corruption while processing IPA statistics,	https://docs.qualcomm.com/pr	O-QUA-WSA8-200125/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			when there are no active clients registered. **CVE ID: CVE-2024-21464**	oduct/publicresources/security bulletin/january-2025-bulletin.html	
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1795
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1796
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1797
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1799
Buffer Copy without Checking Size of Input ('Classic Buffer	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/security bulletin/january-2025-	O-QUA-WSA8-200125/1800

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Overflow')				bulletin.html	
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1801
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1802
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1803
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1804
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1805
Product: wsa8845h_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1806
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is	https://docs.qualcomm.com/product/publicresources/security	O-QUA-WSA8-200125/1807

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	bulletin/january-2025-bulletin.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1808
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1809
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1810
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1811
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1812
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1813
Buffer Over-	06-Jan-2025	7.5	Transient DOS can occur	https://docs.qu	O-QUA-WSA8-

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
read			when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	alcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	200125/1814
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1815
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command IOCTL calls. **CVE ID: CVE-2024-33059**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1816
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1817
Product: wsa8845_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	8.4	Memory corruption while processing IPA statistics, when there are no active clients registered. **CVE ID: CVE-2024-21464**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1818
Use After Free	06-Jan-2025	7.8	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise. **CVE ID: CVE-2024-45553**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1819
Buffer Copy without	06-Jan-2025	7.8	Memory corruption while processing IOCTL call	https://docs.qualcomm.com/pr	O-QUA-WSA8-200125/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			invoked from user-space to verify non extension FIPS encryption and decryption functionality. **CVE ID: CVE-2024-45547**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space. **CVE ID: CVE-2024-45546**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1821
Buffer Over-read	06-Jan-2025	7.8	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call. **CVE ID: CVE-2024-45548**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1822
Improper Validation of Array Index	06-Jan-2025	7.8	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls. **CVE ID: CVE-2024-45550**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to read board data. **CVE ID: CVE-2024-45541**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1824
Stack-based Buffer Overflow	06-Jan-2025	7.8	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver. **CVE ID: CVE-2024-45542**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1825
Buffer Over-read	06-Jan-2025	7.5	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length. **CVE ID: CVE-2024-45558**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1826
Use After Free	06-Jan-2025	6.7	Memory corruption while processing frame command	https://docs.qualcomm.com/pr	O-QUA-WSA8-200125/1827

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

* stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IOCTL calls. **CVE ID: CVE-2024-33059**	oduct/publicresources/securitybulletin/january-2025-bulletin.html	
Use of Out-of-range Pointer Offset	06-Jan-2025	6.7	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls, **CVE ID: CVE-2024-33041**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1828
Use After Free	06-Jan-2025	6.7	Memory corruption while invoking IOCTL calls to unmap the DMA buffers. **CVE ID: CVE-2024-33055**	https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2025-bulletin.html	O-QUA-WSA8-200125/1829

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

* stands for all versions