https://nciipc.gov.in/

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 – 15 Dec 2024 Vol. 11 No. 23

Table of Content

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 1000projects					
Product: attendance_tracking_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	7.3	A vulnerability classified as critical has been found in 1000 Projects Attendance Tracking Management System 1.0. Affected is an unknown function of the file /admin/check_admin_login.php. The manipulation of the argument admin_user_name 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-2024-12497**	N/A	A-100-ATTE-201224/1
Product: beauty_parlour_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Beauty Parlour Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/edit-customer-detailed.php. The manipulation of the argument name leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Other	N/A	A-100-BEAU-201224/2

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
			parameters might be affected as well. **CVE ID : CVE-2024-12234**		
Product: library_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /showbook.php. The manipulation of the argument q 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-2024-12187**	N/A	A-100-LIBR-201224/3
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2024	7.3	A vulnerability was found in 1000 Projects Library Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /brains/stu.php. The manipulation of the argument useri 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-2024-12188**	N/A	A-100-LIBR-201224/4
Vendor: Adobe					
Product: bridge					
Affected Version(s): * Up to (excluding) 14.1.4					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53955**	https://helpx.adobe.com/security/products/bridge/apsb24-103.html	A-ADO-BRID-201224/5
Affected Version(s): 15.0					
Integer Underflow (Wrap or Wraparound)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53955**	https://helpx.adobe.com/security/products/bridge/apsb24-103.html	A-ADO-BRID-201224/6
Product: experience_manager					
Affected Version(s): * Up to (excluding) 2024.11.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52827**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52828**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/8
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52829**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/9
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52830**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-53960**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/11
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52832**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/12
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52834**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52835**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/14
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52836**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/15
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/16

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52841**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52842**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/17
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52843**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52845**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52846**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52847**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/21
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52848**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52849**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52850**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/24
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52851**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52852**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/26
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52853**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/27
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/28

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52854**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52855**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/29
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52857**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/30
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/31

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the page containing the vulnerable field. **CVE ID : CVE-2024-52858**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52859**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/32
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. **CVE ID : CVE-2024-52860**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/33
Improper Neutralization of	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored	https://helpx.adobe.com	A-ADO-EXPE-201224/34

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52861**	/security/products/experience-manager/apsb24-69.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52862**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/35
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52864**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/36
Improper Neutralization of	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored	https://helpx.adobe.com	A-ADO-EXPE-201224/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52991**	/security/products/experience-manager/apsb24-69.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52992**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/38
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52993**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/39
Improper Neutralization of	10-Dec-2024	4.6	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored	https://helpx.adobe.com	A-ADO-EXPE-201224/40

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52865**	/security/products/experience-manager/apsb24-69.html	
Improper Input Validation	10-Dec-2024	3.5	Adobe Experience Manager versions 6.5.21 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-52831**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/41
Affected Version(s): * Up to (excluding) 6.5.22.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52827**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/42

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52828**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/43
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52829**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/44
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52830**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/45

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-53960**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52832**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52834**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52835**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/49
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52836**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/50
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52841**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/51

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52842**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/52
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52843**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/53
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52845**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/54

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52846**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/55
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52847**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/56
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52848**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52849**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/58
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52850**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/59
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52851**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52852**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/61
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52853**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/62
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52854**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/63

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52855**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/64
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52857**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52858**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/66

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52859**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/67
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be exploited by an attacker to execute arbitrary code in the context of the victim's browser session. By manipulating a DOM element through a crafted URL or user input, the attacker can inject malicious scripts that run when the page is rendered. User interaction is required for exploitation, as a victim must visit a malicious link or input data into a vulnerable web application. **CVE ID : CVE-2024-52860**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/68
Improper Neutralization of Input During Web Page Generation	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-201224/69

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52861**	manager/apsb24-69.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52862**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/70
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52864**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/71
Improper Neutralization of Input During Web Page Generation	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-201224/72

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52991**	manager/apsb24-69.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52992**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/73
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Dec-2024	5.4	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52993**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/74
Improper Neutralization of Input During Web Page Generation	10-Dec-2024	4.6	Adobe Experience Manager versions 6.5.21 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a privileged attacker to inject malicious	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPE-201224/75

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. **CVE ID : CVE-2024-52865**	manager/apsb24-69.html	
Improper Input Validation	10-Dec-2024	3.5	Adobe Experience Manager versions 6.5.21 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-52831**	https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html	A-ADO-EXPE-201224/76
Product: framemaker					
Affected Version(s): * Up to (excluding) 2020.7					
Stack-based Buffer Overflow	10-Dec-2024	7.8	Adobe Framemaker versions 2020.7, 2022.5 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53959**	https://helpx.adobe.com/security/products/framemaker/apsb24-106.html	A-ADO-FRAM-201224/77
Affected Version(s): From (including) 2022 Up to (excluding) 2022.5					
Stack-based	10-Dec-2024	7.8	Adobe Framemaker versions 2020.7, 2022.5 and earlier are affected by a Stack-based Buffer	https://helpx.adobe.com/securit	A-ADO-FRAM-201224/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53959**	y/products/framemaker/apsb24-106.html	
Product: premiere_pro					
Affected Version(s): * Up to (excluding) 24.6.4					
Heap-based Buffer Overflow	10-Dec-2024	7.8	Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53956**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html	A-ADO-PREM-201224/79
Affected Version(s): 25.0					
Heap-based Buffer Overflow	10-Dec-2024	7.8	Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53956**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html	A-ADO-PREM-201224/80
Product: substance_3d_modeler					
Affected Version(s): * Up to (including) 1.14.1					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Heap-based Buffer Overflow	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-52999**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/81
Out-of-bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53000**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/82
Out-of-bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53001**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/83
Out-of-bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/produ	A-ADO-SUBS-201224/84

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53002**	cts/substance3d-modeler/apsb24-102.html	
Out-of-bounds Write	10-Dec-2024	7.8	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53003**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/85
Out-of-bounds Read	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53004**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/86
Out-of-bounds Read	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR.	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24	A-ADO-SUBS-201224/87

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53005**	-102.html	
NULL Pointer Dereference	10-Dec-2024	5.5	Substance3D - Modeler versions 1.14.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53006**	https://helpx.adobe.com/security/products/substance3d-modeler/apsb24-102.html	A-ADO-SUBS-201224/88
Product: substance_3d_painter					
Affected Version(s): * Up to (excluding) 10.1.2					
Heap-based Buffer Overflow	10-Dec-2024	7.8	Substance3D - Painter versions 10.1.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53957**	https://helpx.adobe.com/security/products/substance3d_painter/apsb24-105.html	A-ADO-SUBS-201224/89
Out-of-bounds Write	10-Dec-2024	7.8	Substance3D - Painter versions 10.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in	https://helpx.adobe.com/security/produ	A-ADO-SUBS-201224/90

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53958**	cts/substance3d_painter/apsb24-105.html	
Vendor: anisha					
Product: farmacia					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in code-projects Farmacia 1.0. It has been rated as critical. This issue affects some unknown processing of the file /visualizar-usuario.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12492**	N/A	A-ANI-FARM-201224/91
Vendor: anujk305					
Product: medical_card_generation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2024	4.8	PhpGurukul Medical Card Generation System v1.0 is vulnerable to Cross Site Scripting (XSS) in /admin/search-medicalcard.php via the searchdata parameter. **CVE ID : CVE-2024-48703**	N/A	A-ANU-MEDI-201224/92
Vendor: Apple					
Product: safari					
Affected Version(s): * Up to (excluding) 18.1					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. **CVE ID : CVE-2024-44212**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565, https://support.apple.com/en-us/121566, https://support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	A-APP-SAFA-201224/93
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839,	A-APP-SAFA-201224/94

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.	A-APP-SAFA-201224/95

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-	A-APP-SAFA-201224/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-	A-APP-SAFA-201224/97

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121846	
Vendor: cjbi					
Product: wetech-cms					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12479**	N/A	A-CJB-WETE-201224/98
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument con leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and	N/A	A-CJB-WETE-201224/99

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12480**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\UserDao.java. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12481**	N/A	A-CJB-WETE-201224/100
Relative Path Traversal	12-Dec-2024	4.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms-master\wetech-basic-common\src\main\java\tech\wetech\basic\util\BackupFileUtil.java of the component Database Backup Handler. The manipulation of the argument name leads to path traversal: '../filedir'.	N/A	A-CJB-WETE-201224/101

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12482**		
Affected Version(s): 1.1					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12479**	N/A	A-CJB-WETE-201224/102
Improper Neutralization of Special Elements in Output Used by a Downstream Component	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument con leads to	N/A	A-CJB-WETE-201224/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Injection')			sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12480**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\UserDao.java. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12481**	N/A	A-CJB-WETE-201224/104
Relative Path Traversal	12-Dec-2024	4.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms-master\wetech-basic-common\src\main\java\tech\wetech\basic\util\BackupFileUtil.java of the component Database	N/A	A-CJB-WETE-201224/105

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Backup Handler. The manipulation of the argument name leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12482**		
Affected Version(s): 1.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2 and classified as critical. This issue affects the function searchTopicByKeyword of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument keyword leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12479**	N/A	A-CJB-WETE-201224/106
Improper Neutralization of Special Elements in Output Used by a Downstrea	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been classified as critical. Affected is the function searchTopic of the file wetech-cms-master\wetech-	N/A	A-CJB-WETE-201224/107

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			core\src\main\java\tech\wetech\cms\dao\TopicDao.java. The manipulation of the argument con leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12480**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been declared as critical. Affected by this vulnerability is the function findUser of the file wetech-cms-master\wetech-core\src\main\java\tech\wetech\cms\dao\UserDao.java. The manipulation of the argument searchValue/gId/rId leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12481**	N/A	A-CJB-WETE-201224/108
Relative Path Traversal	12-Dec-2024	4.3	A vulnerability was found in cjbi wetech-cms 1.0/1.1/1.2. It has been rated as problematic. Affected by this issue is the function backup of the file wetech-cms-master\wetech-basic-	N/A	A-CJB-WETE-201224/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			common\src\main\java\tech\wetech\basic\util\BackupFileUtil.java of the component Database Backup Handler. The manipulation of the argument name leads to path traversal: '../filedir'. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2024-12482**		
Vendor: classcms					
Product: classcms					
Affected Version(s): 4.8					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2024	2.4	A vulnerability classified as problematic was found in ClassCMS 4.8. Affected by this vulnerability is an unknown functionality of the file /index.php/admin of the component Model Management Page. The manipulation of the argument URL leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12503**	N/A	A-CLA-CLAS-201224/110
Vendor: code-projects					
Product: admin_dashboard					
Affected Version(s): 1.0					
Improper Neutralizat	09-Dec-2024	3.5	A vulnerability was found in code-projects Admin	N/A	A-COD-ADMI-201224/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			Dashboard 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /vendor_management.php. The manipulation of the argument username leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting product names. **CVE ID : CVE-2024-12359**		
Product: farmacia					
Affected Version(s): 1.0					
Improper Neutralizat ion of Special Elements in Output Used by a Downstrea m Componen t ('Injection')	01-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in code-projects Farmacia 1.0. This affects an unknown part of the file /visualizar-produto.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-2024-12007**	N/A	A-COD-FARM-201224/112
Product: hotel_management_system					
Affected Version(s): 1.0					
Improper Restriction of Operations within the Bounds of	05-Dec-2024	5.3	A vulnerability has been found in code-projects Hotel Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the	N/A	A-COD-HOTE-201224/113

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			component Administrator Login Password Handler. The manipulation of the argument Str2 leads to stack-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12185**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-Dec-2024	5.3	A vulnerability was found in code-projects Hotel Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file hotelnew.c of the component Available Room Handler. The manipulation of the argument admin_entry leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12186**	N/A	A-COD-HOTE-201224/114
Vendor: codezips					
Product: technical_discussion_forum					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstrea	12-Dec-2024	7.3	A vulnerability classified as critical was found in Codezips Technical Discussion Forum 1.0. This vulnerability affects unknown code of the file /signuppost.php. The manipulation of the	N/A	A-COD-TECH-201224/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well. **CVE ID : CVE-2024-12484**		
Vendor: datax-web_project					
Product: datax-web					
Affected Version(s): 2.1.1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-Dec-2024	6.3	A vulnerability was found in WeiYe-Jing datax-web 2.1.1. It has been classified as critical. This affects an unknown part of the file /api/job/add/. The manipulation of the argument glueSource leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12358**	N/A	A-DAT-DATA-201224/116
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): * Up to (excluding) 5.7.116					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability classified as problematic has been found in DedeCMS 5.7.116. Affected is an unknown function of the file /member/article_add.php. The manipulation of the argument body leads to cross site scripting. It is possible to launch the attack remotely. The exploit	N/A	A-DED-DEDE-201224/117

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. **CVE ID : CVE-2024-12180**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability classified as problematic was found in DedeCMS 5.7.116. Affected by this vulnerability is an unknown functionality of the file /member/uploads_add.php of the component SWF File Handler. The manipulation of the argument mediatype leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12181**	N/A	A-DED-DEDE-201224/118
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Dec-2024	3.5	A vulnerability, which was classified as problematic, has been found in DedeCMS 5.7.116. Affected by this issue is some unknown functionality of the file /member/soft_add.php. The manipulation of the argument body leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12182**	N/A	A-DED-DEDE-201224/119
Improper Neutralization of Input During Web Page Generation	04-Dec-2024	3.5	A vulnerability, which was classified as problematic, was found in DedeCMS 5.7.116. This affects the function RemoveXSS of the file /plus/carbuyaction.php of the component HTTP POST Request Handler. The	N/A	A-DED-DEDE-201224/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			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-2024-12183**		
Vendor: fabian					
Product: online_class_and_exam_scheduling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability, which was classified as critical, has been found in code-projects Online Class and Exam Scheduling System 1.0. This issue affects some unknown processing of the file /pages/department.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12485**	N/A	A-FAB-ONLI-201224/121
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in code-projects Online Class and Exam Scheduling System 1.0. Affected is an unknown function of the file /pages/rank_update.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	N/A	A-FAB-ONLI-201224/122

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-12486		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability has been found in code-projects Online Class and Exam Scheduling System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /pages/room_update.php. The manipulation of the argument 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-2024-12487**	N/A	A-FAB-ONLI-201224/123
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /pages/subject_update.php. The manipulation of the argument id 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-2024-12488**	N/A	A-FAB-ONLI-201224/124
Improper Neutralization of Special Elements in Output Used by a Downstrea	12-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been classified as critical. This affects an unknown part of the file /pages/term.php. The manipulation of the	N/A	A-FAB-ONLI-201224/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
m Component ('Injection')			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-2024-12489**		
Vendor: fabianros					
Product: online_notice_board					
Affected Version(s): 1.0					
Improper Access Control	05-Dec-2024	7.3	A vulnerability was found in code-projects Online Notice Board up to 1.0 and classified as critical. This issue affects some unknown processing of the file /registration.php of the component Profile Picture Handler. The manipulation of the argument img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12233**	N/A	A-FAB-ONLI-201224/126
Vendor: GFI					
Product: archiver					
Affected Version(s): * Up to (excluding) 15.7					
N/A	12-Dec-2024	9.8	GFI Archiver Telerik Web UI Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability.	N/A	A-GFI-ARCH-201224/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The specific flaw exists within the product installer. The issue results from the use of a vulnerable version of Telerik Web UI. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-24041. **CVE ID : CVE-2024-11948**		
Deserialization of Untrusted Data	12-Dec-2024	8.8	GFI Archiver Core Service Deserialization of Untrusted Data Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is required to exploit this vulnerability. The specific flaw exists within the Core Service, which listens on TCP port 8017 by default. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-24029. **CVE ID : CVE-2024-11947**	N/A	A-GFI-ARCH-201224/128
Deserialization of Untrusted Data	12-Dec-2024	8.8	GFI Archiver Store Service Deserialization of Untrusted Data Remote Code Execution Vulnerability.	N/A	A-GFI-ARCH-201224/129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is required to exploit this vulnerability. The specific flaw exists within the Store Service, which listens on TCP port 8018 by default. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-24331. **CVE ID : CVE-2024-11949**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 131.0.6778.139					
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	Type Confusion in V8 in Google Chrome prior to 131.0.6778.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-12381**	https://chromereleases.googleblog.com/2024/12/stable-channel-update-for-desktop_10.html	A-GOO-CHRO-201224/130
Use After Free	12-Dec-2024	8.8	Use after free in Translate in Google Chrome prior to 131.0.6778.139 allowed a	https://chromereleases.g	A-GOO-CHRO-201224/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2024-12382**	oogleblog.com/2024/12/stable-channel-update-for-desktop_10.html	
Vendor: gstreamer_project					
Product: gstreamer					
Affected Version(s): * Up to (excluding) 1.24.10					
Out-of-bounds Write	12-Dec-2024	7.5	GStreamer is a library for constructing graphs of media-handling components. An OOB-write vulnerability has been identified in the gst_ssa_parse_remove_override_codes function of the gstssaparse.c file. This function is responsible for parsing and removing SSA (SubStation Alpha) style override codes, which are enclosed in curly brackets ({}). The issue arises when a closing curly bracket "}" appears before an opening curly bracket "{" in the input string. In this case, memmove() incorrectly duplicates a substring. With each successive loop iteration, the size passed to memmove() becomes progressively larger (strlen(end+1)), leading to a write beyond the allocated memory bounds. This vulnerability is fixed in 1.24.10.	https://gitlab.freedesktop.org/gstreamer/gstreamer/-/merge_requests/8036.patch, https://gstreamer.freedesktop.org/security/sa-2024-0023.html	A-GST-GSTR-201224/132

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-47541		
Out-of-bounds Read	12-Dec-2024	7.5	GStreamer is a library for constructing graphs of media-handling components. A null pointer dereference has been discovered in the id3v2_read_synch_uint function, located in id3v2.c. If id3v2_read_synch_uint is called with a null work->hdr.frame_data, the pointer guint8 *data is accessed without validation, resulting in a null pointer dereference. This vulnerability can result in a Denial of Service (DoS) by triggering a segmentation fault (SEGV). This vulnerability is fixed in 1.24.10. **CVE ID : CVE-2024-47542**	https://gitlab.freedesktop.org/gstreamer/gstreamer/-/merge_requests/8033.patch, https://gstreamer.freedesktop.org/security/sa-2024-0008.html	A-GST-GSTR-201224/133
Vendor: IBM					
Product: cognos_controller					
Affected Version(s): 11.0.0					
Unrestricted Upload of File with Dangerous Type	03-Dec-2024	8	IBM Cognos Controller 11.0.0 and 11.0.1 could be vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks.	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/134

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-40691		
Use of Hard-coded Credentials	03-Dec-2024	7.5	IBM Cognos Controller 11.0.0 and 11.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. **CVE ID : CVE-2024-41777**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/135
Cross-Site Request Forgery (CSRF)	03-Dec-2024	6.5	IBM Cognos Controller 11.0.0 and 11.0.1	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID : CVE-2024-41776**		
Cleartext Transmission of Sensitive Information	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID : CVE-2021-29892**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/137
Use of a Broken or Risky Cryptographic Algorithm	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2024-41775**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/138
Unrestricted Upload of File with Dangerous Type	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1 could be vulnerable to malicious file upload by not validating the type of file uploaded to Journal entry attachments. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victims for performing further attacks. **CVE ID : CVE-2024-25019**		
Unrestricted Upload of File with Dangerous Type	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to malicious file upload by allowing unrestricted filetype attachments in the Journal entry page. Attackers can make use of this weakness and upload malicious executable files into the system and can be sent to victims for performing further attacks. **CVE ID : CVE-2024-25020**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/140
Exposure of Sensitive System Information to an Unauthorized Control Sphere	03-Dec-2024	5.3	IBM Cognos Controller 11.0.0 and 11.0.1 exposes server details that could allow an attacker to	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtain information of the application environment to conduct further attacks. **CVE ID : CVE-2024-25035**		
Authentication Bypass Using an Alternate Path or Channel	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user with local access to bypass security allowing users to circumvent restrictions imposed on input fields. **CVE ID : CVE-2024-25036**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/142
Insufficient Type Distinction	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user to upload insecure files, due to insufficient file type distinction. **CVE ID : CVE-2024-45676**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/143
Affected Version(s): 11.0.1					
Unrestricted Upload of File with	03-Dec-2024	8	IBM Cognos Controller 11.0.0 and 11.0.1	https://www.ibm.com/s	A-IBM-COGN-201224/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			could be vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks. **CVE ID : CVE-2024-40691**	upport/pages/node/7177220	
Use of Hard-coded Credentials	03-Dec-2024	7.5	IBM Cognos Controller 11.0.0 and 11.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. **CVE ID : CVE-2024-41777**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/145
Cross-Site Request Forgery (CSRF)	03-Dec-2024	6.5	IBM Cognos Controller 11.0.0 and 11.0.1	https://www.ibm.com/support/pages/n	A-IBM-COGN-201224/146

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. **CVE ID : CVE-2024-41776**	ode/7177220	
Cleartext Transmission of Sensitive Information	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. **CVE ID : CVE-2021-29892**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/147
Use of a Broken or Risky Cryptographic Algorithm	03-Dec-2024	5.9	IBM Cognos Controller 11.0.0 and 11.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. **CVE ID : CVE-2024-41775**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/148
Unrestricted Upload of	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1	https://www.ib	A-IBM-COGN-201224/149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
File with Dangerous Type			could be vulnerable to malicious file upload by not validating the type of file uploaded to Journal entry attachments. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to victims for performing further attacks. **CVE ID : CVE-2024-25019**	m.com/support/pages/node/7177220	
Unrestricted Upload of File with Dangerous Type	03-Dec-2024	5.5	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to malicious file upload by allowing unrestricted filetype attachments in the Journal entry page. Attackers can make use of this weakness and upload malicious executable files into the system and can be sent to	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			victims for performing further attacks. **CVE ID : CVE-2024-25020**		
Exposure of Sensitive System Information to an Unauthorized Control Sphere	03-Dec-2024	5.3	IBM Cognos Controller 11.0.0 and 11.0.1 exposes server details that could allow an attacker to obtain information of the application environment to conduct further attacks. **CVE ID : CVE-2024-25035**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/151
Authentication Bypass Using an Alternate Path or Channel	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user with local access to bypass security allowing users to circumvent restrictions imposed on input fields. **CVE ID : CVE-2024-25036**	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/152
Insufficient Type Distinction	03-Dec-2024	4.3	IBM Cognos Controller 11.0.0 and 11.0.1	https://www.ibm.com/support/pages/node/7177220	A-IBM-COGN-201224/153

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an authenticated user to upload insecure files, due to insufficient file type distinction. **CVE ID : CVE-2024-45676**		
Vendor: ivanti					
Product: automation					
Affected Version(s): * Up to (excluding) 2024.4.0.1					
Incorrect Default Permissions	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Automation before version 2024.4.0.1 allows a local authenticated attacker to achieve local privilege escalation. **CVE ID : CVE-2024-9845**	https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Automation-CVE-2024-9845	A-IVA-AUTO-201224/154
Product: security_controls					
Affected Version(s): * Up to (excluding) 2024.4.1					
Incorrect Default Permissions	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Security Controls before version 2024.4.1 allows a local authenticated attacker to achieve local privilege escalation. **CVE ID : CVE-2024-10251**	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Security-Controls-iSec-CVE-	A-IVA-SECU-201224/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-10251	
Product: workspace_control					
Affected Version(s): From (including) 10.18.30.0 Up to (excluding) 10.18.40.0					
Incorrect Default Permissions	11-Dec-2024	7.8	Under specific circumstances, insecure permissions in Ivanti Workspace Control before version 10.18.40.0 allows a local authenticated attacker to achieve local privilege escalation. **CVE ID : CVE-2024-8496**	https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Workspace-Control-IWC-CVE-2024-8496	A-IVA-WORK-201224/156
Vendor: jwillber					
Product: jfinalcms					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2024	6.3	A vulnerability was found in JFinalCMS 1.0. It has been rated as critical. Affected by this issue is the function update of the file \src\main\java\com\cms\controller\admin\TemplateController.java of the component Template Handler. The manipulation of the argument content leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	N/A	A-JWI-JFIN-201224/157

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-12350		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2024	6.3	A vulnerability classified as critical has been found in JFinalCMS 1.0. This affects the function findPage of the file src\main\java\com\cms\entity\ContentModel.java of the component File Content Handler. The manipulation of the argument name leads to sql injection. It is possible to initiate the attack remotely. **CVE ID : CVE-2024-12351**	N/A	A-JWI-JFIN-201224/158
Cross-Site Request Forgery (CSRF)	09-Dec-2024	4.3	A vulnerability was found in JFinalCMS 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/tag/save. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12349**	N/A	A-JWI-JFIN-201224/159
Vendor: lopalopa					
Product: e-learning_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command	09-Dec-2024	9.8	A SQL Injection vulnerability was found in /teacher_signup.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL command to get unauthorized database	N/A	A-LOP-E-LE-201224/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			access via the firstname, lastname, and class_id parameters. **CVE ID : CVE-2024-54920**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2024	8.8	A SQL Injection vulnerability was found in /search_class.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the school_year parameter. **CVE ID : CVE-2024-54926**	N/A	A-LOP-E-LE-201224/161
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2024	7.2	KASHIPARA E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_subject.php. **CVE ID : CVE-2024-54929**	N/A	A-LOP-E-LE-201224/162
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2024	7.2	A SQL Injection was found in /admin/edit_user.php of kashipara E-learning Management System v1.0, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the firstname, lastname, and username parameters. **CVE ID : CVE-2024-54922**	N/A	A-LOP-E-LE-201224/163
Improper Neutralization of Special	09-Dec-2024	7.2	Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection	N/A	A-LOP-E-LE-201224/164

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			in /admin/delete_student.php. **CVE ID : CVE-2024-54930**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	09-Dec-2024	7.2	Kashipara E-learning Management System v1.0 is vulnerable to SQL Injection in /admin/delete_content.php. **CVE ID : CVE-2024-54933**	N/A	A-LOP-E-LE-201224/165
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2024	5.4	A Stored Cross-Site Scripting (XSS) vulnerability was found in /send_message.php of Kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter. **CVE ID : CVE-2024-54936**	N/A	A-LOP-E-LE-201224/166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Dec-2024	5.4	A Stored Cross Site Scripting (XSS) was found in /teacher_avatar.php of kashipara E-learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary java script via the filename parameter. **CVE ID : CVE-2024-54919**	N/A	A-LOP-E-LE-201224/167
Improper Neutralization of Input During	09-Dec-2024	5.4	A Stored Cross-Site Scripting (XSS) vulnerability was found in /send_message_teacher_to_student.php of kashipara E-	N/A	A-LOP-E-LE-201224/168

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			learning Management System v1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the my_message parameter. **CVE ID : CVE-2024-54935**		
N/A	09-Dec-2024	5.3	A Directory Listing issue was found in Kashipara E-Learning Management System v1.0, which allows remote attackers to access sensitive files and directories via /admin/assets. **CVE ID : CVE-2024-54937**	N/A	A-LOP-E-LE-201224/169
Vendor: mayurik					
Product: advocate_office_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Dec-2024	3.5	A vulnerability, which was classified as problematic, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file /control/client_data.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12536**	N/A	A-MAY-ADVO-201224/170
Product: best_house_rental_management_system					
Affected Version(s): 1.0					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Control of File Name or Path	09-Dec-2024	4.3	A vulnerability was found in SourceCodester Best House Rental Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /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-2024-12357**	N/A	A-MAY-BEST-201224/171
Vendor: online_class_and_exam_scheduling_system_project					
Product: online_class_and_exam_scheduling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-Dec-2024	6.3	A vulnerability was found in code-projects Online Class and Exam Scheduling System 1.0. It has been rated as critical. This issue affects some unknown processing of the file class_update.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12360**	N/A	A-ONL-ONLI-201224/172
Vendor: openrobotics					
Product: robot_operating_system					
Affected Version(s): 2					
Improper Preservati	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open	N/A	A-OPE-ROBO-201224/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on of Permissions			Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via the dyn_param_handler_ component. **CVE ID : CVE-2024-41644**		
Improper Preservation of Permissions	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2__amcl. **CVE ID : CVE-2024-41645**	N/A	A-OPE-ROBO-201224/174
Improper Preservation of Permissions	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_dwb_controller. **CVE ID : CVE-2024-41646**	N/A	A-OPE-ROBO-201224/175
N/A	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_mppi_controller. **CVE ID : CVE-2024-41647**	N/A	A-OPE-ROBO-201224/176
Improper Preservation of Permissions	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the	N/A	A-OPE-ROBO-201224/177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nav2_regulated_pure_pursuit_controller. **CVE ID : CVE-2024-41648**		
Improper Preservation of Permissions	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the executor_thread_. **CVE ID : CVE-2024-41649**	N/A	A-OPE-ROBO-201224/178
Improper Preservation of Permissions	06-Dec-2024	9.8	Insecure Permissions vulnerability in Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble allows an attacker to execute arbitrary code via a crafted script to the nav2_costmap_2d. **CVE ID : CVE-2024-41650**	N/A	A-OPE-ROBO-201224/179
NULL Pointer Dereference	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component computeControl(). **CVE ID : CVE-2024-44853**	N/A	A-OPE-ROBO-201224/180
NULL Pointer Dereference	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component smoothPlan(). **CVE ID : CVE-2024-44854**	N/A	A-OPE-ROBO-201224/181
NULL Pointer	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was	N/A	A-OPE-ROBO-201224/182

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dereference			discovered to contain a NULL pointer dereference via the component nav2_navfn_planner(). **CVE ID : CVE-2024-44855**		
NULL Pointer Dereference	06-Dec-2024	7.5	Open Robotics Robotic Operating System 2 ROS2 navigation2 v.humble was discovered to contain a NULL pointer dereference via the component nav2_smac_planner(). **CVE ID : CVE-2024-44856**	N/A	A-OPE-ROBO-201224/183
Vendor: phpgurukul					
Product: complaint_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2024	7.3	A vulnerability classified as critical has been found in PHPGurukul Complaint Management System 1.0. Affected is an unknown function of the file /admin/user-search.php. The manipulation of the argument search 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-2024-12228**	N/A	A-PHP-COMP-201224/184
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	05-Dec-2024	7.3	A vulnerability classified as critical was found in PHPGurukul Complaint Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/complaint-search.php. The manipulation of the	N/A	A-PHP-COMP-201224/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			argument search 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-2024-12229**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Dec-2024	7.3	A vulnerability, which was classified as critical, has been found in PHPGurukul Complaint Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/subcategory.php. The manipulation of the argument category 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-2024-12230**	N/A	A-PHP-COMP-201224/186
Product: covid_19_testing_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Dec-2024	6.1	A Reflected Cross Site Scripting (XSS) vulnerability was found in /covidtms/registered-user-testing.php in PHPGurukul COVID 19 Testing Management System 1.0 which allows remote attackers to execute arbitrary code via the regmobilenumber parameter. **CVE ID : CVE-2024-55268**	N/A	A-PHP-COVI-201224/187
Vendor: Progress					
Product: whatsup_gold					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 24.0.1					
N/A	02-Dec-2024	9.8	In WhatsUp Gold versions released before 2024.0.1, a remote unauthenticated attacker could leverage this vulnerability to execute code in the context of the service account. **CVE ID : CVE-2024-46909**	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	A-PRO-WHAT-201224/188
Incorrect Use of Privileged APIs	02-Dec-2024	9.8	In WhatsUp Gold versions released before 2024.0.1, a remote unauthenticated attacker could leverage NmAPI.exe to create or change an existing registry value in registry path HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Ipswitch\. **CVE ID : CVE-2024-8785**	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	A-PRO-WHAT-201224/189
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated lower-privileged user (at least Network Manager permissions required) to achieve privilege escalation to the admin account. **CVE ID : CVE-2024-46905**	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	A-PRO-WHAT-201224/190
Improper Neutralizat	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a	https://commun	A-PRO-WHAT-201224/191

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an SQL Command ('SQL Injection')			SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. **CVE ID : CVE-2024-46906**	ity.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. **CVE ID : CVE-2024-46907**	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	A-PRO-WHAT-201224/192
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Dec-2024	8.8	In WhatsUp Gold versions released before 2024.0.1, a SQL Injection vulnerability allows an authenticated low-privileged user (at least Report Viewer permissions required) to achieve privilege escalation to the admin account. **CVE ID : CVE-2024-46908**	https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024	A-PRO-WHAT-201224/193
Vendor: razormist					
Product: phone_contact_manager_system					
Affected Version(s): 1.0					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	5.3	A vulnerability, which was classified as critical, was found in SourceCodester Phone Contact Manager System 1.0. Affected is the function UserInterface::MenuDisplayStart of the component User Menu. The manipulation leads to buffer overflow. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12354**	N/A	A-RAZ-PHON-201224/194
Improper Input Validation	09-Dec-2024	3.3	A vulnerability, which was classified as problematic, has been found in SourceCodester Phone Contact Manager System 1.0. This issue affects the function UserInterface::MenuDisplayStart of the component User Menu. The manipulation of the argument name leads to improper input validation. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12353**	N/A	A-RAZ-PHON-201224/195
Improper Input Validation	09-Dec-2024	3.3	A vulnerability has been found in SourceCodester Phone Contact Manager System 1.0 and classified as problematic. Affected by this vulnerability is the function ContactBook::adding of the file ContactBook.cpp. The manipulation leads to	N/A	A-RAZ-PHON-201224/196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12355**		
Vendor: Rockwellautomation					
Product: arena_simulation					
Affected Version(s): * Up to (including) 16.20.03					
Out-of-bounds Write	05-Dec-2024	7.8	An “out of bounds write” code execution vulnerability exists in the Rockwell Automation Arena® that could allow a threat actor to write beyond the boundaries of allocated memory in a DOE file. If exploited, a threat actor could leverage this vulnerability to execute arbitrary code. To exploit this vulnerability, a legitimate user must execute the malicious code crafted by the threat actor. **CVE ID : CVE-2024-11156**	https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1713.html	A-ROC-AREN-201224/197
Out-of-bounds Read	05-Dec-2024	7.8	An “out of bounds read” code execution vulnerability exists in the Rockwell Automation Arena® that could allow a threat actor to craft a DOE file and force the software to read	https://www.rockwellautomation.com/en-us/trust-center/security-	A-ROC-AREN-201224/198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			beyond the boundaries of an allocated memory. If exploited, a threat actor could leverage this vulnerability to execute arbitrary code. To exploit this vulnerability, a legitimate user must execute the malicious code crafted by the threat actor. **CVE ID : CVE-2024-12130**	advisories/advisory.SD1713.html	
Vendor: ujcms					
Product: ujcms					
Affected Version(s): * Up to (excluding) 9.6.3					
Improper Authorization	12-Dec-2024	3.7	A vulnerability classified as problematic has been found in Dromara UJCMS up to 9.6.3. This affects an unknown part of the file /users/id of the component User ID Handler. The manipulation leads to authorization bypass. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12483**	N/A	A-UJC-UJCM-201224/199
Hardware					
Vendor: Qualcomm					
Product: 205_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-205_-201224/200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-205_-201224/201
Product: 215_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-215_-201224/202
Product: 315_5g_iot_modem					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-315_-201224/203
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-315_-201224/204
Product: 9205_lte_modem					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-9205-201224/205
Product: 9206_lte_modem					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-9206-201224/206
Product: 9207_lte_modem					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-9207-201224/207
Product: apq8017					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-APQ8-201224/208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: apq8037					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-APQ8-201224/209
Product: aqt1000					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-AQT1-201224/210
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-AQT1-201224/211

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: ar8035					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-AR80-201224/212
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-AR80-201224/213
Product: c-v2x_9150					
Affected Version(s): -					
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicreso	H-QUA-C-V2-201224/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	urces/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-C-V2-201224/215
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-C-V2-201224/216
Product: csrb31024					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-CSRB-201224/217

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: fastconnect_6200					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/218
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/219
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-FAST-201224/220

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/221
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/222
Product: fastconnect_6700					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-FAST-201224/223

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/224
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/225
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/226

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/227
Product: fastconnect_6800					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/228
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/230
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/231
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/232
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	H-QUA-FAST-201224/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/234
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/235
Product: fastconnect_6900					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-FAST-201224/236

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/237
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/238
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-FAST-201224/239

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
				cember-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/240
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/241
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/242

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/243
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/244
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/245
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-FAST-201224/246

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/247
Product: fastconnect_7800					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/248
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro duct/pu	H-QUA-FAST-201224/249

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/250
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/251
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-FAST-201224/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/253
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/254
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/255

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/256
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FAST-201224/257
Product: flight_rb5_5g_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FLIG-201224/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FLIG-201224/259
Product: fsm10055					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-FSM1-201224/260
Product: fsm10056					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-FSM1-201224/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: home_hub_100_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-HOME-201224/262
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-HOME-201224/263
Product: immersive_home_214_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-IMME-201224/264

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: immersive_home_216_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IMME-201224/265
Product: immersive_home_316_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IMME-201224/266
Product: immersive_home_318_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-IMME-201224/267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Product: immersive_home_3210_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IMME-201224/268
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IMME-201224/269
Product: immersive_home_326_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	H-QUA-IMME-201224/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IMME-201224/271
Product: ipq5010					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/272
Product: ipq5028					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/273
Product: ipq5300					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/274
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/275
Product: ipq5302					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/276
Product: ipq5312					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/277
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ipq5332					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/279
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ5-201224/280
Product: ipq6000					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-IPQ6-201224/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: ipq6005					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ6-201224/282
Product: ipq6010					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ6-201224/283
Product: ipq6018					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-IPQ6-201224/284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: ipq6028					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ6-201224/285
Product: ipq8064					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/286
Product: ipq8065					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	H-QUA-IPQ8-201224/287

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: ipq8068					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/288
Product: ipq8070					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/289
Product: ipq8070a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/290
Product: ipq8071					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/291
Product: ipq8071a					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-IPQ8-201224/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: ipq8072					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/293
Product: ipq8072a					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/294
Product: ipq8074					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-IPQ8-201224/295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: ipq8074a					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/296
Product: ipq8076					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/297
Product: ipq8076a					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/298
Product: ipq8078					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/299
Product: ipq8078a					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-IPQ8-201224/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: ipq8173					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/301
Product: ipq8174					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ8-201224/302
Product: ipq9008					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-IPQ9-201224/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ9-201224/304
Product: ipq9554					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ9-201224/305
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-IPQ9-201224/306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: ipq9570					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ9-201224/307
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ9-201224/308
Product: ipq9574					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-IPQ9-201224/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-IPQ9-201224/310
Product: mdm8207					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MDM8-201224/311
Product: mdm9205s					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-MDM9-201224/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: mdm9250					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MDM9-201224/313
Product: mdm9628					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MDM9-201224/314
Product: mdm9650					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MDM9-201224/315
Product: msm8108					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/316
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/317
Product: msm8209					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/318
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/319
Product: msm8608					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/320

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/321
Product: msm8909w					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-MSM8-201224/322
Product: pm8937					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-PM89-201224/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: pmp8074					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-PMP8-201224/324
Product: qam8255p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/325
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QAM8-201224/326

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/327
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/328
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qam8295p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/330
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/331
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/333
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/334
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/335
Product: qam8620p					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/336
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/337
Product: qam8650p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/338

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/339
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/340
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/341
Product: qam8775p					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/342
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/343
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAM8-201224/344
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	H-QUA-QAM8-201224/345

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qamsrv1h					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/346
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/347
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-QAMS-201224/348

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/349
Product: qamsrv1m					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/350
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	H-QUA-QAMS-201224/351

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/352
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QAMS-201224/353
Product: qca0000					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QCA0-201224/354

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA0-201224/355
Product: qca1062					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA1-201224/356
Product: qca1064					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https://docs.qualcomm.com/product/pu	H-QUA-QCA1-201224/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43050	blicresources/securitybulletin/december-2024-bulletin.html	
Product: qca2062					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/358
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/359
Product: qca2064					
Affected Version(s): -					
Stack-based	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https://docs.qualcomm.c	H-QUA-QCA2-201224/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			test command inside WLAN driver. **CVE ID : CVE-2024-43050**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/361
Product: qca2065					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/362
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https://docs.qualcomm.com/pro	H-QUA-QCA2-201224/363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. **CVE ID : CVE-2024-43053**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca2066					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/364
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA2-201224/365
Product: qca4004					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qua	H-QUA-QCA4-201224/366

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca4024					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA4-201224/367
Product: qca6164					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6174					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/369
Product: qca6174a					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/370
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/371

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/372
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/373
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/374
Product: qca6310					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/375
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/376
Product: qca6320					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6335					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/378
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/379
Product: qca6391					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/381
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/382
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/383

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/384
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/385
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/386
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-QCA6-201224/387

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/388
Product: qca6420					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/389
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-QCA6-201224/390

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/391
Product: qca6421					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/392
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-QCA6-201224/393

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/394
Product: qca6426					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/395
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QCA6-201224/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/397
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/398
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/399

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/400
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/401
Product: qca6428					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6430					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/403
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/404
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6431					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/406
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/407
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6436					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/409
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/410
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/412
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/413
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/414

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/415
Product: qca6438					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/416
Product: qca6554a					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/418
Product: qca6564					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/419
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6564a					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/421
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/422
Product: qca6564au					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QCA6-201224/423

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/424
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/425
Product: qca6574					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-QCA6-201224/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/427
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/428
Product: qca6574a					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/429

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/430
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/431
Product: qca6574au					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/432

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/433
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/434
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/435

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/436
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/437
Product: qca6584au					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/438

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/439
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/440
Product: qca6595					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/441

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/442
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/443
Product: qca6595au					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/445
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/446
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/447
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	H-QUA-QCA6-201224/448

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6678aq					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/449
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/450
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-QCA6-201224/451

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/452
Product: qca6688aq					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/453
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-QCA6-201224/454

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/455
Product: qca6694					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/456
Product: qca6696					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/pro	H-QUA-QCA6-201224/457

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/458
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/459
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QCA6-201224/460

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33036	lletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/461
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/462
Product: qca6698aq					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QCA6-201224/463

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/464
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/465
Product: qca6777aq					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/467
Product: qca6787aq					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/468
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/469

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca6797aq					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/470
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA6-201224/471
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-QCA6-201224/472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qca8072					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/473
Product: qca8075					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/474
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QCA8-201224/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: qca8081					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/476
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/477
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-QCA8-201224/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qca8082					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/479
Product: qca8084					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/480
Product: qca8085					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/publicreso	H-QUA-QCA8-201224/481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	urces/securitybulletin/december-2024-bulletin.html	
Product: qca8337					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/482
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/483
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QCA8-201224/484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/485
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA8-201224/486
Product: qca8386					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QCA8-201224/487

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qca9377					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA9-201224/488
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCA9-201224/489
Product: qca9379					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicreso	H-QUA-QCA9-201224/490

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: qcc2073					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC2-201224/491
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC2-201224/492
Improper Restriction of Operations within the Bounds of	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QCC2-201224/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer				curitybulletin/december-2024-bulletin.html	
Product: qcc2076					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC2-201224/494
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC2-201224/495
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QCC2-201224/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qcc710					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC7-201224/497
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCC7-201224/498
Product: qcf8000					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso	H-QUA-QCF8-201224/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: qcf8001					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCF8-201224/500
Product: qcm2150					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM2-201224/501
Product: qcm4325					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM4-201224/502
Product: qcm5430					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM5-201224/503
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM5-201224/504
Product: qcm6490					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM6-201224/505
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM6-201224/506
Product: qcm8550					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM8-201224/507

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM8-201224/508
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM8-201224/509
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCM8-201224/510
Product: qcn5124					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN5-201224/511
Product: qcn6224					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/512
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/513
Product: qcn6274					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/514
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/515
Product: qcn6402					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qcn6412					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/517
Product: qcn6422					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN6-201224/518
Product: qcn6432					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QCN6-201224/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: qcn7605					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN7-201224/520
Product: qcn7606					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN7-201224/521
Product: qcn9000					
Affected Version(s): -					
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-QCN9-201224/522

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: qcn9011					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/523
Product: qcn9012					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/524
Product: qcn9024					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/525
Product: qcn9074					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/526
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/528
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/529
Product: qcn9160					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/530
Product: qcn9274					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/531
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/532
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCN9-201224/533
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https://docs.qua	H-QUA-QCN9-201224/534

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qcs2290					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS2-201224/535
Product: qcs410					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/537
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/538
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/539
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	H-QUA-QCS4-201224/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qcs4290					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/541
Product: qcs4490					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS4-201224/542
Product: qcs5430					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS5-201224/543
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS5-201224/544
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS5-201224/545
Product: qcs610					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/546
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/547
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/548
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-QCS6-201224/549

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/550
Product: qcs6125					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/551
Product: qcs6490					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/552
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/553
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS6-201224/554
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/pro	H-QUA-QCS6-201224/555

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qcs7230					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS7-201224/556
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS7-201224/557
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	H-QUA-QCS7-201224/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS7-201224/559
Product: qcs8155					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/560
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-QCS8-201224/561

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: qcs8250					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/562
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/563
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QCS8-201224/564

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/565
Product: qcs8550					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/566
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QCS8-201224/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/568
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS8-201224/569
Product: qcs9100					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QCS9-201224/570

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QCS9-201224/571
Product: qdu1000					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDU1-201224/572
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-QDU1-201224/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qdu1010					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDU1-201224/574
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDU1-201224/575
Product: qdu1110					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin	H-QUA-QDU1-201224/576

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDU1-201224/577
Product: qdu1210					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDU1-201224/578
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QDU1-201224/579

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: qdx1010					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDX1-201224/580
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDX1-201224/581
Product: qdx1011					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QDX1-201224/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QDX1-201224/583
Product: qep8111					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QEP8-201224/584
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QEP8-201224/585

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qet4101					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QET4-201224/586
Product: qfw7114					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QFW7-201224/587
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-QFW7-201224/588

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QFW7-201224/589
Product: qfw7124					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QFW7-201224/590
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QFW7-201224/591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QFW7-201224/592
Product: qrb5165m					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRB5-201224/593
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QRB5-201224/594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qrb5165n					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRB5-201224/595
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRB5-201224/596
Product: qru1032					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-QRU1-201224/597

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRU1-201224/598
Product: qru1052					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRU1-201224/599
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-QRU1-201224/600

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: qru1062					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRU1-201224/601
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QRU1-201224/602
Product: qsm8250					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-QSM8-201224/603

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSM8-201224/604
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSM8-201224/605
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-QSM8-201224/606

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSM8-201224/607
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSM8-201224/608
Product: qsm8350					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-QSM8-201224/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSM8-201224/610
Product: qsw8573					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QSW8-201224/611
Product: qts110					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-QTS1-201224/612

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qxm8083					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-QXM8-201224/613
Product: robotics_rb3_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-ROBO-201224/614
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-ROBO-201224/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: robotics_rb5_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-ROBO-201224/616
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-ROBO-201224/617
Product: sa2150p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-SA21-201224/618

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa4150p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA41-201224/619
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA41-201224/620
Product: sa4155p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA41-201224/621
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA41-201224/622
Product: sa6145p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/623

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/624
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/625
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/626
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	H-QUA-SA61-201224/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa6150p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/628
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/629
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel	https://docs.qualcomm.com/product/pu	H-QUA-SA61-201224/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	blicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/631
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/632
Product: sa6155					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-SA61-201224/633

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/634
Product: sa6155p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/635
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SA61-201224/636

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/637
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/638
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SA61-201224/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA61-201224/640
Product: sa7255p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA72-201224/641
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SA72-201224/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA72-201224/643
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA72-201224/644
Product: sa7775p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SA77-201224/645

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA77-201224/646
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA77-201224/647
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA77-201224/648
Product: sa8145p					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/649
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/650
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/651
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to	https://docs.qua	H-QUA-SA81-201224/652

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/653
Product: sa8150p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/654
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	H-QUA-SA81-201224/655

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/656
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/657
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SA81-201224/658

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33037	curitybulletin/december-2024-bulletin.html	
Product: sa8155					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/659
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/660
Product: sa8155p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-SA81-201224/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/662
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/663
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SA81-201224/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/665
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/666
Product: sa8195p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SA81-201224/667

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/668
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/669
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/670

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/671
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA81-201224/672
Product: sa8255p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/673

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/674
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/675
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/676
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	H-QUA-SA82-201224/677

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa8295p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/678
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/679
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-SA82-201224/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/681
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA82-201224/682
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SA82-201224/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: sa8530p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/684
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/685
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SA85-201224/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/687
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/688
Product: sa8540p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SA85-201224/689

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/690
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/691
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA85-201224/693
Product: sa8620p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/694
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/696
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/697
Product: sa8650p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/698

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/699
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/700
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA86-201224/701
Product: sa8770p					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/702
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/703
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/704
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	H-QUA-SA87-201224/705

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa8775p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/706
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/707
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-SA87-201224/708

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA87-201224/709
Product: sa9000p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA90-201224/710
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	H-QUA-SA90-201224/711

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA90-201224/712
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA90-201224/713
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SA90-201224/714

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA90-201224/715
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SA90-201224/716
Product: sc8180x					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SC81-201224/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC81-201224/718
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC81-201224/719
Product: sc8380xp					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SC83-201224/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC83-201224/721
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC83-201224/722
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC83-201224/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC83-201224/724
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SC83-201224/725
Product: sd460					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD46-201224/726
Product: sd660					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD66-201224/727
Product: sd662					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD66-201224/728
Product: sd670					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SD67-201224/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD67-201224/730
Product: sd675					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD67-201224/731
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SD67-201224/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sd730					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD73-201224/733
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD73-201224/734
Product: sd835					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SD83-201224/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: sd855					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD85-201224/736
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD85-201224/737
Product: sd865_5g					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SD86-201224/738

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD86-201224/739
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD86-201224/740
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SD86-201224/741

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD86-201224/742
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD86-201224/743
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD86-201224/744
Product: sd888					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD88-201224/745
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD88-201224/746
Product: sdm429w					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/747

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/748
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/749
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/750
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https://docs.qualcomm.com/pro	H-QUA-SDM4-201224/751

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. **CVE ID : CVE-2024-43050**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/752
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDM4-201224/753
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SDM4-201224/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: sdx20m					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX2-201224/755
Product: sdx55					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/756
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-SDX5-201224/757

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/758
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/759
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SDX5-201224/760

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/761
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/762
Product: sdx57m					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SDX5-201224/763

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX5-201224/764
Product: sdx61					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX6-201224/765
Product: sdx65m					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SDX6-201224/766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX6-201224/767
Product: sdx71m					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SDX7-201224/768
Product: sd_455					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SD_4-201224/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: sd_675					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD_6-201224/770
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD_6-201224/771
Product: sd_8cx					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-SD_8-201224/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD_8-201224/773
Product: sd_8_gen1_5g					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SD_8-201224/774
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-SD_8-201224/775

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: sg4150p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SG41-201224/776
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SG41-201224/777
Product: sg8275p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-SG82-201224/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SG82-201224/779
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SG82-201224/780
Product: sm4125					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-SM41-201224/781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Product: sm4635					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM46-201224/782
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM46-201224/783
Product: sm6250					
Affected Version(s): -					
Improper Validation	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	https://docs.qualcomm.c	H-QUA-SM62-201224/784

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Array Index			**CVE ID : CVE-2024-33044**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM62-201224/785
Product: sm6250p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM62-201224/786
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-SM62-201224/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm6370					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM63-201224/788
Product: sm7250p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM72-201224/789
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qua	H-QUA-SM72-201224/790

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM72-201224/791
Product: sm7315					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM73-201224/792
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	H-QUA-SM73-201224/793

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm7325p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM73-201224/794
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM73-201224/795
Product: sm8550p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM85-201224/796
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM85-201224/797
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM85-201224/798
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/pro	H-QUA-SM85-201224/799

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm8635					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM86-201224/800
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM86-201224/801
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	H-QUA-SM86-201224/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM86-201224/803
Product: sm8750					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM87-201224/804
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources	H-QUA-SM87-201224/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM87-201224/806
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM87-201224/807
Product: sm8750p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SM87-201224/808

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SM87-201224/809
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SM87-201224/810
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SM87-201224/811

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: smart_audio_200_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SMAR-201224/812
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SMAR-201224/813
Product: smart_audio_400_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SMAR-201224/814

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: snapdragon_1100_wearable_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/815
Product: snapdragon_1200_wearable_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/816
Product: snapdragon_208_processor					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/817

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/818
Product: snapdragon_210_processor					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/819
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_212_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/821
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/822
Product: snapdragon_425_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_427_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/824
Product: snapdragon_429_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/825
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qua	H-QUA-SNAP-201224/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/827
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/828
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/829

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43050	urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/830
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/831
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/832

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_430_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/833
Product: snapdragon_435_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/834
Product: snapdragon_439_mobile_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_460_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/836
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/837
Product: snapdragon_480\+_5g_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/838

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/839
Product: snapdragon_480_5g_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/840
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/841

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_4_gen_1_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/842
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/843
Product: snapdragon_4_gen_2_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	H-QUA-SNAP-201224/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_630_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/845
Product: snapdragon_636_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/846
Product: snapdragon_660_mobile_platform					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/847
Product: snapdragon_662_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/848
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/849

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_665_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/850
Product: snapdragon_670_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/851
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/852

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_675_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/853
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/854
Product: snapdragon_678_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/856
Product: snapdragon_680_4g_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/857
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_685_4g_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/859
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/860
Product: snapdragon_690_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/861

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/862
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/863
Product: snapdragon_695_5g_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/865
Product: snapdragon_710_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/866
Product: snapdragon_712_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: snapdragon_720g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/868
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/869
Product: snapdragon_730g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/871
Product: snapdragon_730_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/872
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/873

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_732g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/874
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/875
Product: snapdragon_750g_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/877
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/878
Product: snapdragon_765g_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/879

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/880
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/881
Product: snapdragon_765_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/883
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/884
Product: snapdragon_768g_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/886
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/887
Product: snapdragon_778g\+_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/888

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/889
Product: snapdragon_778g_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/890
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: snapdragon_780g_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/892
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/893
Product: snapdragon_782g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/895
Product: snapdragon_7c\+_gen_3_compute					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/896
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin	H-QUA-SNAP-201224/897

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/898
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/899
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_7c_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/901
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/902
Product: snapdragon_7c_gen_2_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/904
Product: snapdragon_820_automotive_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/905
Product: snapdragon_835_mobile_pc_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: snapdragon_845_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/907
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/908
Product: snapdragon_850_mobile_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/910
Product: snapdragon_855\+					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/911
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	H-QUA-SNAP-201224/912

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_855_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/913
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/914
Product: snapdragon_860_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/916
Product: snapdragon_865\+_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/917
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-SNAP-201224/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/919
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/920
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/921

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/922
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/923
Product: snapdragon_865_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/925
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/926
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/927

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/928
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/929
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/930
Product: snapdragon_870_5g_mobile_platform					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/931
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/932
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/933
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/934

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/935
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/936
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: snapdragon_888\+_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/938
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/939
Product: snapdragon_888_5g_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresso	H-QUA-SNAP-201224/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/941
Product: snapdragon_8cx_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/942
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/943

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/944
Product: snapdragon_8cx_gen_2_5g_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/945
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/946

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/947
Product: snapdragon_8cx_gen_3_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/948
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/949

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
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/950
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/951
Product: snapdragon_8c_compute_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/953
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/954
Product: snapdragon_8\+_gen_1_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/955

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_8\+_gen_2_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/956
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/957
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/959
Product: snapdragon_8_gen_1_mobile_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/960
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/962
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/963
Product: snapdragon_8_gen_2_mobile_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/965
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/966
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/967
Product: snapdragon_8_gen_3_mobile_platform					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/968
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/969
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/970

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/971
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/972
Product: snapdragon_ar2_gen_1_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/973

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/974
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/975
Product: snapdragon_auto_4g_modem					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/977
Product: snapdragon_auto_5g_modem-rf					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/978
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/979
Product: snapdragon_auto_5g_modem-rf_gen_2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/980
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/981
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/982
Product: snapdragon_w5\+_gen_1_wearable_platform					
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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/983
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/984
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/985
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	H-QUA-SNAP-201224/986

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/987
Product: snapdragon_wear_1300_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/988
Product: snapdragon_wear_2100_platform					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/989
Product: snapdragon_wear_2500_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/990
Product: snapdragon_wear_3100_platform					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_wear_4100\+_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/992
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/993
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_x12_lte_modem					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/995
Product: snapdragon_x20_lte_modem					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/996
Product: snapdragon_x24_lte_modem					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SNAP-201224/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/998
Product: snapdragon_x35_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/999
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/1000

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: snapdragon_x50_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1001
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1002
Product: snapdragon_x55_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-SNAP-201224/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1004
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1005
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/1006

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1007
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1008
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1009

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_x5_lte_modem					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1010
Product: snapdragon_x62_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1011
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/1012

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: snapdragon_x65_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1013
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1014
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SNAP-201224/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_x70_modem-rf_system					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1016
Product: snapdragon_x72_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1017
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1019
Product: snapdragon_x75_5g_modem-rf_system					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1020
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SNAP-201224/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1022
Product: snapdragon_xr1_platform					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1023
Product: snapdragon_xr2\+_gen_1_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SNAP-201224/1024

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1025
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1026
Product: snapdragon_xr2_5g_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SNAP-201224/1027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1028
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1029
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1030

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1031
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1032
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SNAP-201224/1033
Product: srv1h					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1034
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1035
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1036
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	H-QUA-SRV1-201224/1037

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: srv1l					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1038
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1039
Product: srv1m					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1040
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1041
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SRV1-201224/1042
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	H-QUA-SRV1-201224/1043

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
			handle is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: ssg2115p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SSG2-201224/1044
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SSG2-201224/1045
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	H-QUA-SSG2-201224/1046

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: ssg2125p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SSG2-201224/1047
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SSG2-201224/1048
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso	H-QUA-SSG2-201224/1049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: sw5100					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1050
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1051
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	https://docs.qualcomm.com/product/publicresources/se	H-QUA-SW51-201224/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33039	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1053
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1054
Product: sw5100p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-SW51-201224/1055

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1056
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1057
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-SW51-201224/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SW51-201224/1059
Product: sxr1120					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR1-201224/1060
Product: sxr1230p					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-SXR1-201224/1061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR1-201224/1062
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR1-201224/1063
Product: sxr2130					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-SXR2-201224/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1065
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1066
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1067

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1068
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1069
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1070
Product: sxr2230p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1071
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1072
Product: sxr2250p					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1073

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-SXR2-201224/1074
Product: talynplus					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-TALY-201224/1075
Product: video_collaboration_vc1_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-VIDE-201224/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1077
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1078
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1080
Product: video_collaboration_vc3_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1081
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1082

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1083
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1084
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1085
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-VIDE-201224/1086

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1087
Product: video_collaboration_vc5_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1088
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-VIDE-201224/1089

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1090
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VIDE-201224/1091
Product: vision_intelligence_300_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-VISI-201224/1092

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VISI-201224/1093
Product: vision_intelligence_400_platform					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VISI-201224/1094
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-VISI-201224/1095

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VISI-201224/1096
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-VISI-201224/1097
Product: wcd9306					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WCD9-201224/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcd9326					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1099
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1100
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-WCD9-201224/1101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: wcd9330					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1102
Product: wcd9335					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1103
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/se	H-QUA-WCD9-201224/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1105
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1106
Product: wcd9340					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WCD9-201224/1107

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1108
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1109
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WCD9-201224/1110

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcd9341					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1111
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1112
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WCD9-201224/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1114
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1115
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1116

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1117
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1118
Product: wcd9360					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1119

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1120
Product: wcd9370					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1121
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1123
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1124
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1125
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/pro	H-QUA-WCD9-201224/1126

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1127
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1128
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WCD9-201224/1129

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcd9371					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1130
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1131
Product: wcd9375					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	H-QUA-WCD9-201224/1132

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1133
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1134
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-WCD9-201224/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1136
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1137
Product: wcd9378					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WCD9-201224/1138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcd9380					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1139
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1140
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WCD9-201224/1141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1142
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1143
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1145
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1146
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1147
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-WCD9-201224/1148

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1149
Product: wcd9385					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1150
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	H-QUA-WCD9-201224/1151

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1152
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1153
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-WCD9-201224/1154

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1155
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1156
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9390					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1158
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1159
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1160

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1161
Product: wcd9395					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1162
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1164
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCD9-201224/1165
Product: wcn3610					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1166
Product: wcn3615					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1167
Product: wcn3620					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1168
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1169

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
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1170
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1171
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1172
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https://docs.qualcomm.com/pro	H-QUA-WCN3-201224/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. **CVE ID : CVE-2024-43053**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1174
Product: wcn3660b					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1175
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	H-QUA-WCN3-201224/1176

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1177
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1178
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-WCN3-201224/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1180
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1181
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1182

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1183
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1184
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1185
Product: wcn3680					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1186
Product: wcn3680b					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1187
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1189
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1190
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1191
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	H-QUA-WCN3-201224/1192

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: wcn3950					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1193
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1194
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel	https://docs.qualcomm.com/pro duct/pu	H-QUA-WCN3-201224/1195

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	blicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1196
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1197
Product: wcn3980					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources	H-QUA-WCN3-201224/1198

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1199
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1200
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	H-QUA-WCN3-201224/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1202
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1203
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1204

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wcn3988					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1205
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1206
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1207

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1208
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1209
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1210
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	H-QUA-WCN3-201224/1211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1212
Product: wcn3990					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1213
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	H-QUA-WCN3-201224/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1215
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN3-201224/1216
Product: wcn3999					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	H-QUA-WCN3-201224/1217

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: wcn6740					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN6-201224/1218
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN6-201224/1219
Product: wcn6755					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	H-QUA-WCN6-201224/1220

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN6-201224/1221
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN6-201224/1222
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WCN6-201224/1223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcn7860					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1224
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1225
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-WCN7-201224/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1227
Product: wcn7861					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1228
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de cember-	H-QUA-WCN7-201224/1229

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1230
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1231
Product: wcn7880					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WCN7-201224/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1233
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1234
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1235
Product: wcn7881					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1236
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1237
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WCN7-201224/1238
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https://docs.qua	H-QUA-WCN7-201224/1239

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: wsa8810					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1240
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1241
Stack-based	02-Dec-2024	7.8	Memory corruption when invalid input is passed to	https://docs.qualcomm.c	H-QUA-WSA8-201224/1242

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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			invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1243
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1244
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicresources/se	H-QUA-WSA8-201224/1245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1246
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1247
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1248

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wsa8815					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1249
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1250
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1252
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1253
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1255
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1256
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1257
Product: wsa8830					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1258
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1259
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1260
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic	https://docs.qualcomm.com/pro	H-QUA-WSA8-201224/1261

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			private command inside WLAN driver. **CVE ID : CVE-2024-43049**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1262
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1263
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WSA8-201224/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1265
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1266
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1267

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1268
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1269
Product: wsa8832					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1271
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1272
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1274
Product: wsa8835					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1275
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1277
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1278
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1279
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https://docs.qualcomm.com/pro	H-QUA-WSA8-201224/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1281
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1282
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WSA8-201224/1283

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1284
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1285
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wsa8840					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1287
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1288
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	H-QUA-WSA8-201224/1289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1290
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1291
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1293
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1294
Product: wsa8845					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1295

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1296
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1297
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1298
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https://docs.qualcomm.com/pro	H-QUA-WSA8-201224/1299

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. **CVE ID : CVE-2024-43050**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1300
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1301
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	H-QUA-WSA8-201224/1302

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wsa8845h					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1303
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1304
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	H-QUA-WSA8-201224/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1306
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1307
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1308

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1309
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	H-QUA-WSA8-201224/1310
Vendor: totolink					
Product: ex1800t					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	4.3	A vulnerability classified as problematic was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This vulnerability affects the function sub_40662C of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed	N/A	H-TOT-EX18-201224/1311

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 the public and may be used. **CVE ID : CVE-2024-12352**		
Vendor: Tp-link					
Product: vn020_f3v					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.5	A vulnerability classified as critical has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected is an unknown function of the file /control/WANIPConnection of the component SOAP Request Handler. The manipulation of the argument NewConnectionType leads to buffer overflow. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12343**	https://www.tp-link.com/	H-TP--VN02-201224/1312
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in TP-Link VN020 F3v(T) TT_V6.2.1021. This affects an unknown part of the component FTP USER Command Handler. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12344**	N/A	H-TP--VN02-201224/1313
Operating System					
Vendor: Apple					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ipados					
Affected Version(s): * Up to (excluding) 17.7.3					
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-IPAD-241224/1314
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https://support.apple.com/en-us/1218	O-APP-IPAD-241224/1315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	37, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://	O-APP-IPAD-241224/1316

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 disclosure of process memory. **CVE ID : CVE-2024-54486**	support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121839, https://support.apple.co	O-APP-IPAD-241224/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. **CVE ID : CVE-2024-44201**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-IPAD-241224/1318
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2,	https://support.apple.com/en-	O-APP-IPAD-241224/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state.	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838,	O-APP-IPAD-241224/1320

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-54510	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Affected Version(s): * Up to (excluding) 18.1					
N/A	12-Dec-2024	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. **CVE ID : CVE-2024-44299**	https://support.apple.com/en-us/121563	O-APP-IPAD-241224/1321
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one	https://support.apple.com/en-us/121563, https://support.	O-APP-IPAD-241224/1322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			origin may be sent to another origin. **CVE ID : CVE-2024-44212**	apple.com/en-us/121565, https://support.apple.com/en-us/121566, https://support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to read sensitive location information. **CVE ID : CVE-2024-44200**	https://support.apple.com/en-us/121563	O-APP-IPAD-241224/1323
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1. An app may be able to determine a user's current location. **CVE ID : CVE-2024-44290**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565	O-APP-IPAD-241224/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-IPAD-241224/1325
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2,	https://support.apple.com/en-us/121837,	O-APP-IPAD-241224/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.	O-APP-IPAD-241224/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. **CVE ID : CVE-2024-54526**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-	O-APP-IPAD-241224/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121843, https://support.apple.com/en-us/121844	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-	O-APP-IPAD-241224/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121844	
N/A	12-Dec-2024	4.2	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 18.2 and iPadOS 18.2. Muting a call while ringing may not result in mute being enabled. **CVE ID : CVE-2024-54503**	https://support.apple.com/en-us/121837	O-APP-IPAD-241224/1330
Affected Version(s): * Up to (including) 17.7.3					
N/A	12-Dec-2024	2.4	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. **CVE ID : CVE-2024-54485**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838	O-APP-IPAD-241224/1331
Affected Version(s): From (including) 18.0 Up to (excluding) 18.1					
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. **CVE ID : CVE-2024-44201**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/1218	O-APP-IPAD-241224/1332

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				40, https://support.apple.com/en-us/121842	
Affected Version(s): From (including) 18.0 Up to (excluding) 18.2					
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-	O-APP-IPAD-241224/1333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-IPAD-241224/1334
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https://support.apple.com/en-us/1218	O-APP-IPAD-241224/1335

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	37, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://	O-APP-IPAD-241224/1336

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapping that can be written to. **CVE ID : CVE-2024-54494**	support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.co	O-APP-IPAD-241224/1337

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/1218	O-APP-IPAD-241224/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				42, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	2.4	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. **CVE ID : CVE-2024-54485**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838	O-APP-IPAD-241224/1339
Product: iphone_os					
Affected Version(s): * Up to (excluding) 18.1					
N/A	12-Dec-2024	9.8	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. **CVE ID : CVE-2024-44299**	https://support.apple.com/en-us/121563	O-APP-IPHO-241224/1340
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. **CVE ID : CVE-2024-44201**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/1218	O-APP-IPHO-241224/1341

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				38, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. **CVE ID : CVE-2024-44212**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565, https://support.apple.com/en-us/121566, https://support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	O-APP-IPHO-241224/1342

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to read sensitive location information. **CVE ID : CVE-2024-44200**	https://support.apple.com/en-us/121563	O-APP-IPHO-241224/1343
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1. An app may be able to determine a user's current location. **CVE ID : CVE-2024-44290**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565	O-APP-IPHO-241224/1344
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-	O-APP-IPHO-241224/1345

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844,	O-APP-IPHO-241224/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-IPHO-241224/1347

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-IPHO-241224/1348
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2,	https://support.apple.com/en-us/121837, https://support.	O-APP-IPHO-241224/1349

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-	O-APP-IPHO-241224/1350

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840,	O-APP-IPHO-241224/1351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-IPHO-241224/1352

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. **CVE ID : CVE-2024-54526**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	O-APP-IPHO-241224/1353
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may	https://support.apple.com/en-us/121837, https://support.	O-APP-IPHO-241224/1354

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to access sensitive user data. **CVE ID : CVE-2024-54527**	apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-	O-APP-IPHO-241224/1355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	4.2	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 18.2 and iPadOS 18.2. Muting a call while ringing may not result in mute being enabled. **CVE ID : CVE-2024-54503**	https://support.apple.com/en-us/121837	O-APP-IPHO-241224/1356
N/A	12-Dec-2024	2.4	The issue was addressed by adding additional logic. This issue is fixed in iPadOS 17.7.3, iOS 18.2 and iPadOS 18.2. An attacker with physical access to an iOS device may be able to view notification content from the lock screen. **CVE ID : CVE-2024-54485**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838	O-APP-IPHO-241224/1357
Product: macos					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Integer Underflow (Wrap or Wraparound)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53955**	https://helpx.adobe.com/security/products/bridge/apsb24-103.html	O-APP-MACO-241224/1358
Heap-based Buffer Overflow	10-Dec-2024	7.8	Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53956**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html	O-APP-MACO-241224/1359
Affected Version(s): * Up to (excluding) 13.7.2					
N/A	12-Dec-2024	8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. **CVE ID : CVE-2024-54498**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.	O-APP-MACO-241224/1360

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121842	
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. **CVE ID : CVE-2024-54489**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1361
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2024-54528**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1362
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS	https://support.apple.co	O-APP-MACO-241224/1363

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	m/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/1218	O-APP-MACO-241224/1364

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Race Condition')			mapping that can be written to. **CVE ID : CVE-2024-54494**	38, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54474**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1365

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54477**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1366
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.	O-APP-MACO-241224/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-	O-APP-MACO-241224/1368

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121844	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	O-APP-MACO-241224/1369
Affected Version(s): * Up to (excluding) 15.2					
N/A	12-Dec-2024	9.8	A logic issue was addressed with improved state management. This issue is fixed in macOS Sequoia	https://support.apple.com/en-	O-APP-MACO-241224/1370

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			15.2. An app may be able to elevate privileges. **CVE ID : CVE-2024-54465**	us/121839	
Out-of-bounds Read	12-Dec-2024	9.8	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.2. An attacker may be able to cause unexpected system termination or arbitrary code execution in DCP firmware. **CVE ID : CVE-2024-54506**	https://support.apple.com/en-us/121839	O-APP-MACO-241224/1371
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/1218	O-APP-MACO-241224/1372

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				45, https://support.apple.com/en-us/121846	
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-MACO-241224/1373

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
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2. A malicious app may be able to gain root privileges. **CVE ID : CVE-2024-54515**	https://support.apple.com/en-us/121839	O-APP-MACO-241224/1374
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-MACO-241224/1375

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-MACO-241224/1376
Insertion of Sensitive Information into Log File	12-Dec-2024	5.5	The issue was resolved by sanitizing logging. This issue is fixed in macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54484**	https://support.apple.com/en-us/121839	O-APP-MACO-241224/1377

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54504**	https://support.apple.com/en-us/121839	O-APP-MACO-241224/1378
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-MACO-241224/1379
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.2. An	https://support.apple.com/en-	O-APP-MACO-241224/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to bypass kASLR. **CVE ID : CVE-2024-54531**	us/121839	
N/A	12-Dec-2024	3.3	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.2. Privacy indicators for microphone access may be attributed incorrectly. **CVE ID : CVE-2024-54493**	https://support.apple.com/en-us/121839	O-APP-MACO-241224/1381
Affected Version(s): * Up to (including) 13.7.2					
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. **CVE ID : CVE-2024-54526**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843,	O-APP-MACO-241224/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121844	
Affected Version(s): From (including) 13.0 Up to (excluding) 13.7.2					
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. **CVE ID : CVE-2024-44291**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1383
N/A	12-Dec-2024	6.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A user with screen sharing access may be able to view another user's screen. **CVE ID : CVE-2024-44248**	https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1384
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and	https://support.apple.com/en-us/1215	O-APP-MACO-241224/1385

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. **CVE ID : CVE-2024-44201**	63, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	5.5	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access protected user data. **CVE ID : CVE-2024-44300**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1386
Affected Version(s): From (including) 14.0 Up to (excluding) 14.7.2					
N/A	12-Dec-2024	8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2,	https://support.apple.com/en-us/1218	O-APP-MACO-241224/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. **CVE ID : CVE-2024-54498**	39, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. **CVE ID : CVE-2024-44291**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1388
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. **CVE ID : CVE-2024-54489**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840,	O-APP-MACO-241224/1389

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2024-54528**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1390
N/A	12-Dec-2024	6.5	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A user with screen sharing access may be able to view another user's screen. **CVE ID : CVE-2024-44248**	https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1391
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2,	https://support.apple.com/en-us/121837, https://	O-APP-MACO-241224/1392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.co	O-APP-MACO-241224/1393

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, macOS Ventura 13.7.2, iOS 18.1 and iPadOS 18.1, macOS Sonoma 14.7.2. Processing a malicious crafted file may lead to a denial-of-service. **CVE ID : CVE-2024-44201**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121840, https://support.apple.com/en-	O-APP-MACO-241224/1394

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121842	
N/A	12-Dec-2024	5.5	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access protected user data. **CVE ID : CVE-2024-44300**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1395
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54474**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1396
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS	https://support.apple.com/en-us/1218	O-APP-MACO-241224/1397

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sonoma 14.7.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54477**	39, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://	O-APP-MACO-241224/1398

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	O-APP-MACO-241224/1399
Concurrent Execution	12-Dec-2024	5.1	A race condition was addressed with improved	https://support.	O-APP-MACO-241224/1400

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Affected Version(s): From (including) 14.0 Up to (including) 14.7.2					
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious	https://support.apple.com/en-us/121837, https://support.	O-APP-MACO-241224/1401

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to access private information. **CVE ID : CVE-2024-54526**	apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
Affected Version(s): From (including) 15.0 Up to (excluding) 15.2					
N/A	12-Dec-2024	8.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to break out of its sandbox. **CVE ID : CVE-2024-54498**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.	O-APP-MACO-241224/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121842	
N/A	12-Dec-2024	7.8	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to gain root privileges. **CVE ID : CVE-2024-44291**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1403
N/A	12-Dec-2024	7.8	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Running a mount command may unexpectedly execute arbitrary code. **CVE ID : CVE-2024-54489**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1404
N/A	12-Dec-2024	7.1	A logic issue was addressed with improved restrictions. This issue is fixed in macOS	https://support.apple.co	O-APP-MACO-241224/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to overwrite arbitrary files. **CVE ID : CVE-2024-54528**	m/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/1218	O-APP-MACO-241224/1406

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				42, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	O-APP-MACO-241224/1407

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access protected user data. **CVE ID : CVE-2024-44300**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1408
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access user-sensitive data. **CVE ID : CVE-2024-54474**	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	O-APP-MACO-241224/1409
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may	https://support.apple.com/en-us/121839, https://	O-APP-MACO-241224/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be able to access user-sensitive data. **CVE ID : CVE-2024-54477**	support.apple.com/en-us/121840, https://support.apple.com/en-us/121842	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.co	O-APP-MACO-241224/1411

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. **CVE ID : CVE-2024-54526**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	O-APP-MACO-241224/1412
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS	https://support.apple.com/en-	O-APP-MACO-241224/1413

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state.	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838,	O-APP-MACO-241224/1414

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-54510	https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Product: tvos					
Affected Version(s): * Up to (excluding) 18.1					
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. **CVE ID : CVE-2024-44212**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565, https://support.apple.com/en-us/1215	O-APP-TVOS-241224/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				66, https://support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	
Affected Version(s): * Up to (excluding) 18.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/1218	O-APP-TVOS-241224/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				45, https://support.apple.com/en-us/121846	
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-TVOS-241224/1417

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-TVOS-241224/1418
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously	https://support.apple.com/en-us/121837, https://support.	O-APP-TVOS-241224/1419

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-	O-APP-TVOS-241224/1420

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840,	O-APP-TVOS-241224/1421

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.	O-APP-TVOS-241224/1422

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	O-APP-TVOS-241224/1423
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious	https://support.apple.com/en-us/121837, https://support.apple.co	O-APP-TVOS-241224/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to access private information. **CVE ID : CVE-2024-54526**	m/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/1218	O-APP-TVOS-241224/1425

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
				40, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://	O-APP-TVOS-241224/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Product: visionos					
Affected Version(s): * Up to (excluding) 2.1					
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. **CVE ID : CVE-2024-44212**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565, https://support.apple.com/en-us/121566, https://support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	O-APP-VISI-241224/1427

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-VISI-241224/1428
Access of Resource Using Incompatible Type	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https://support.apple.com/en-us/121837,	O-APP-VISI-241224/1429

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Type Confusion')			macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.	O-APP-VISI-241224/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-	O-APP-VISI-241224/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842,	O-APP-VISI-241224/1432

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory mapping that can be written to. **CVE ID : CVE-2024-54494**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	O-APP-VISI-241224/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	O-APP-VISI-241224/1434
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An	https://support.apple.com/en-us/121837, https://support.	O-APP-VISI-241224/1435

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845	
Product: watchos					
Affected Version(s): * Up to (excluding) 11.1					
Origin Validation Error	12-Dec-2024	5.3	A cookie management issue was addressed with improved state management. This issue is fixed in Safari 18.1, visionOS 2.1, tvOS 18.1, iOS 18.1 and iPadOS 18.1, watchOS 11.1. Cookies belonging to one origin may be sent to another origin. **CVE ID : CVE-2024-44212**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565, https://support.apple.com/en-us/121566, https://	O-APP-WATC-241224/1436

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support.apple.com/en-us/121569, https://support.apple.com/en-us/121571	
N/A	12-Dec-2024	3.3	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1. An app may be able to determine a user's current location. **CVE ID : CVE-2024-44290**	https://support.apple.com/en-us/121563, https://support.apple.com/en-us/121565	O-APP-WATC-241224/1437
Affected Version(s): * Up to (excluding) 11.2					
Out-of-bounds Write	12-Dec-2024	9.8	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54534**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://	O-APP-WATC-241224/1438

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	
Access of Resource Using Incompatible Type ('Type Confusion')	12-Dec-2024	8.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to memory corruption. **CVE ID : CVE-2024-54505**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.co	O-APP-WATC-241224/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121844, https://support.apple.com/en-us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54479**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-	O-APP-WATC-241224/1440

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121845	
N/A	12-Dec-2024	7.5	The issue was addressed with improved memory handling. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, Safari 18.2, iOS 18.2 and iPadOS 18.2. Processing maliciously crafted web content may lead to an unexpected process crash. **CVE ID : CVE-2024-54508**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-us/121845, https://support.apple.com/en-us/121846	O-APP-WATC-241224/1441
N/A	12-Dec-2024	6.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2,	https://support.apple.com/en-us/1218	O-APP-WATC-241224/1442

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted font may result in the disclosure of process memory. **CVE ID : CVE-2024-54486**	37, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.9	A race condition was addressed with additional validation. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An attacker may be able to create a read-only memory	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://	O-APP-WATC-241224/1443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mapping that can be written to. **CVE ID : CVE-2024-54494**	support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. Processing a maliciously crafted image may result in disclosure of process memory. **CVE ID : CVE-2024-54500**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://support.apple.com/en-us/121839, https://support.apple.co	O-APP-WATC-241224/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
N/A	12-Dec-2024	5.5	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 11.2, visionOS 2.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54513**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844, https://support.apple.com/en-	O-APP-WATC-241224/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				us/121845	
N/A	12-Dec-2024	5.5	The issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. A malicious app may be able to access private information. **CVE ID : CVE-2024-54526**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	O-APP-WATC-241224/1446
N/A	12-Dec-2024	5.5	This issue was addressed with improved checks. This issue is fixed in watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and	https://support.apple.com/en-us/1218	O-APP-WATC-241224/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to access sensitive user data. **CVE ID : CVE-2024-54527**	37, https://support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843, https://support.apple.com/en-us/121844	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-Dec-2024	5.1	A race condition was addressed with improved locking. This issue is fixed in iPadOS 17.7.3, watchOS 11.2, tvOS 18.2, macOS Sequoia 15.2, iOS 18.2 and iPadOS 18.2, macOS Ventura 13.7.2, macOS Sonoma 14.7.2. An app may be able to leak sensitive kernel state. **CVE ID : CVE-2024-54510**	https://support.apple.com/en-us/121837, https://support.apple.com/en-us/121838, https://	O-APP-WATC-241224/1448

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				support.apple.com/en-us/121839, https://support.apple.com/en-us/121840, https://support.apple.com/en-us/121842, https://support.apple.com/en-us/121843	
Vendor: Huawei					
Product: harmonyos					
Affected Version(s): 5.0.0					
Uncaught Exception	12-Dec-2024	7.1	Null pointer dereference vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54106**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1449
Improper Input Validation	12-Dec-2024	7.1	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability.	https://consumer.huawei.com/en/support/bullet	O-HUA-HARM-241224/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-54107	in/2024/12/	
Improper Input Validation	12-Dec-2024	6.5	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54108**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1451
Improper Input Validation	12-Dec-2024	6.5	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54109**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1452
N/A	12-Dec-2024	6.5	Process residence vulnerability in abnormal scenarios in the print module Impact: Successful exploitation of this vulnerability may affect power consumption. **CVE ID : CVE-2024-54113**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1453
N/A	12-Dec-2024	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2024-54104**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1454
Improper Privilege Management	12-Dec-2024	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this	https://consumer.huawei.com/en/support/bullet	O-HUA-HARM-241224/1455

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect service confidentiality. **CVE ID : CVE-2024-54110**	in/2024/12/	
Exposure of Sensitive Information to an Unauthorized Actor	12-Dec-2024	6.2	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2024-54117**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1456
Exposure of Sensitive Information to an Unauthorized Actor	12-Dec-2024	6.1	Vulnerability of improper access control in the album module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2024-54103**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1457
Insufficient Verification of Data Authenticity	12-Dec-2024	5.7	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54111**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1458
N/A	12-Dec-2024	5.5	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality. **CVE ID : CVE-2024-54112**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1459
Buffer Copy without Checking Size of	12-Dec-2024	5.1	Read/Write vulnerability in the image decoding module Impact: Successful exploitation of this	https://consumer.huawei.com/en/suppo	O-HUA-HARM-241224/1460

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			vulnerability will affect availability. **CVE ID : CVE-2024-54105**	rt/bulletin/2024/12/	
Improper Check for Unusual or Exceptional Conditions	12-Dec-2024	4.4	Out-of-bounds access vulnerability in playback in the DASH module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54114**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1461
Improper Check for Unusual or Exceptional Conditions	12-Dec-2024	4.3	Out-of-bounds read vulnerability in the DASH module Impact: Successful exploitation of this vulnerability will affect availability. **CVE ID : CVE-2024-54115**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1462
Improper Check for Unusual or Exceptional Conditions	12-Dec-2024	4.3	Out-of-bounds read vulnerability in the M3U8 module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally. **CVE ID : CVE-2024-54116**	https://consumer.huawei.com/en/support/bulletin/2024/12/	O-HUA-HARM-241224/1463
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): * Up to (excluding) 6.11.10					
Double Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/6825cb07b79ffeb1d90ffaa	O-LIN-LINU-241224/1464

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/amd/display: Handle dml allocation failure to avoid crash [Why] In the case where a dml allocation fails for any reason, the current state's dml contexts would no longer be valid. Then subsequent calls dc_state_copy_internal would shallow copy invalid memory and if the new state was released, a double free would occur. [How] Reset dml pointers in new_state to NULL and avoid invalid pointer (cherry picked from commit bcafdc61529a48f6f06355d78eb41b3aeda5296c) **CVE ID : CVE-2024-53133**	7a1227462cdca34ae, https://git.kernel.org/stable/c/874ff59cde8fc525112dda26b501a1bac17dde9f	
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Clear virtualized VMLOAD/VMSAVE on Zen4 client	https://git.kernel.org/stable/c/00c713f84f477a85e524f34aad8fbd11a1c051f0,	O-LIN-LINU-241224/1465

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A number of Zen4 client SoCs advertise the ability to use virtualized VMLOAD/VMSAVE, but using these instructions is reported to be a cause of a random host reboot. These instructions aren't intended to be advertised on Zen4 client so clear the capability. **CVE ID : CVE-2024-53114**	https://git.kernel.org/stable/c/a5ca1dc46a6b610dd4627d8b633d6c84f9724ef0	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: sched/task_stack: fix object_is_on_stack() for KASAN tagged pointers When CONFIG_KASAN_SW_TAGS and CONFIG_KASAN_STACK are enabled, the object_is_on_stack() function may produce incorrect results due to the presence of tags in the obj pointer, while the stack pointer does not have tags. This discrepancy can lead to incorrect stack object detection and subsequently trigger warnings if CONFIG_DEBUG_OBJECTS is also enabled.	https://git.kernel.org/stable/c/fbfe23012cec509dfbe09852019c4e4bb84999d0, https://git.kernel.org/stable/c/fd7b4f9f46d46acbc7af3a439bb0d869efdc5c58	O-LIN-LINU-241224/1466

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Example of the warning: ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated. ------------[cut here]------------ WARNING: CPU: 0 PID: 1 at lib/debugobjects.c:557 __debug_object_init+0x330/0x364 Modules linked in: CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc5 #4 Hardware name: linux,dummy-virt (DT) pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __debug_object_init+0x330/0x364 lr : __debug_object_init+0x330/0x364 sp : ffff800082ea7b40 x29: ffff800082ea7b40 x28: 98ff0000c0164518 x27: 98ff0000c0164534 x26: ffff800082d93ec8 x25: 0000000000000001 x24: 1cff0000c00172a0 x23: 0000000000000000 x22: ffff800082d93ed0 x21: ffff800081a24418		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x20: 3eff800082ea7bb0 x19: efff800000000000 x18: 0000000000000000 x17: 00000000000000ff x16: 0000000000000047 x15: 206b63617473206e x14: 0000000000000018 x13: ffff800082ea7780 x12: 0ffff800082ea78e x11: 0ffff800082ea790 x10: 0ffff800082ea79d x9 : 34d77febe173e800 x8 : 34d77febe173e800 x7 : 0000000000000001 x6 : 0000000000000001 x5 : feff800082ea74b8 x4 : ffff800082870a90 x3 : ffff80008018d3c4 x2 : 0000000000000001 x1 : ffff800082858810 x0 : 0000000000000050 Call trace: __debug_object_init+0x330/0x364 debug_object_init_on_stack+0x30/0x3c schedule_hrtimeout_range_clock+0xac/0x26c schedule_hrtimeout+0x1c/0x30 wait_task_inactive+0x1d4/0x25c		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			kthread_bind_mask+0x28/0x98 init_rescuer+0x1e8/0x280 workqueue_init+0x1a0/0x3cc kernel_init_freeable+0x118/0x200 kernel_init+0x28/0x1f0 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated. ------------[cut here]------------ **CVE ID : CVE-2024-53128**		
Affected Version(s): * Up to (excluding) 6.6.63					
Out-of-bounds Read	02-Dec-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adjust VSDB parser for replay feature At some point, the IEEE ID identification for the replay check in the AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN:	https://git.kernel.org/stable/c/0a326fbc8f72a320051f27328d4d4e7abdfe68d7, https://git.kernel.org/stable/c/16dd2825c23530f2259fc671960a3	O-LIN-LINU-241224/1467

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesync_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 ... [27.821207] Memory state around the buggy address: [27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821268] ==	a65d2af69bd, https://git.kernel.org/stable/c/8db867061f4c76505ad62422b65d666b45289217	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			======================== This is caused because the ID extraction happens outside of the range of the edid lenght. This commit addresses this issue by considering the amd_vsdb_block size. (cherry picked from commit b7e381b1ccd5e778e3d9c44c669ad38439a861d8) **CVE ID : CVE-2024-53108**		
Affected Version(s): * Up to (including) 6.3					
N/A	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is placed on the stack. Neither pcim_iomap_regions() nor the functions it calls copy that string. Should the string later ever be used, this, consequently, causes undefined behavior since the stack frame will by then have disappeared.	https://git.kernel.org/stable/c/0b364cf53b20204e92bac7c6ebd1ee7d3ec62931, https://git.kernel.org/stable/c/5bb287da2d2d5bb8f7376e223b02edb16998982e, https://git.kernel.org/stable/c/d372dd0	O-LIN-LINU-241224/1468

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fix the bug by allocating the strings on the heap through devm_kasprintf(). **CVE ID : CVE-2024-53126**	9cfbf1324f54cbffd81fcaf6cdf3e608e	
Affected Version(s): 6.12					
Double Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Handle dml allocation failure to avoid crash [Why] In the case where a dml allocation fails for any reason, the current state's dml contexts would no longer be valid. Then subsequent calls dc_state_copy_internal would shallow copy invalid memory and if the new state was released, a double free would occur. [How] Reset dml pointers in new_state to NULL and avoid invalid pointer	https://git.kernel.org/stable/c/6825cb07b79ffeb1d90ffaa7a1227462cdca34ae, https://git.kernel.org/stable/c/874ff59cde8fc525112dda26b501a1bac17dde9f	O-LIN-LINU-241224/1469

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
			(cherry picked from commit bcafdc61529a48f6f06355d78eb41b3aeda5296c) **CVE ID : CVE-2024-53133**		
Use After Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST=y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] ============================= WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W ----------------------------- net/core/dev.c:876 RCU-list traversed in non-reader section!! other info that might help us debug this:	https://git.kernel.org/stable/c/05656a66592759242c74063616291b7274d11b2f, https://git.kernel.org/stable/c/ad975697211f4f2c4ce61c3ba524fd14d88ceab8, https://git.kernel.org/stable/c/eb72e7fcc83987d5d5595b43222f23b295d5de7f	O-LIN-LINU-241224/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	rcu_scheduler_active = 2, debug_locks = 1 1 lock held by sctp_hello/31495: #0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}-{0:0}, at: sctp_bind (./arch/x86/include/asm/jump_label.h:27 net/sctp/socket.c:315) sctp stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5-virtme #1216 Tainted: [W]=WARN Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) lockdep_rcu_suspicious (kernel/locking/lockdep.c:6822) dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7)) sctp_v6_available (net/sctp/ipv6.c:701) sctp sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp sctp_bind (net/sctp/socket.c:320) sctp		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inet6_bind_sk (net/ipv6/af_inet6.c:465) ? security_socket_bind (security/security.c:4581 (discriminator 1)) __sys_bind (net/socket.c:1848 net/socket.c:1869) ? do_user_addr_fault (./include/linux/rcupdate.h:347 ./include/linux/rcupdate.h:880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) ? do_user_addr_fault (./arch/x86/include/asm/preempt.h:84 (discriminator 13) ./include/linux/rcupdate.h:98 (discriminator 13) ./include/linux/rcupdate.h:882 (discriminator 13) ./include/linux/mm.h:729 (discriminator 13) arch/x86/mm/fault.c:1340 (discriminator 13)) __x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1) arch/x86/entry/common.c:83 (discriminator 1)) entry_SYSCALL_64_after_hwframe		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48 All code ======== 0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00 mov 0xc8c39(%rip),%rdx # 0xc8c43 a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx) f: b8 ff ff ff ff mov $0xffffffff,%eax 14: eb bd jmp 0xffffffffffffffd3 16: 66 2e 0f 1f 84 00 00 cs nopw 0x0(%rax,%rax,1) 1d: 00 00 00 20: 0f 1f 00 nopl (%rax) 23: b8 31 00 00 00 mov $0x31,%eax 28: 0f 05 syscall 2a:* 48 3d 01 f0 ff ff cmp		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			$0xfffffffffffff001,%rax <-- trapping instruction 30: 73 01 jae 0x33 32: c3 ret 33: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c43 3a: f7 d8 neg %eax 3c: 64 89 01 mov %eax,%fs:(%rcx) 3f: 48 rex.W Code starting with the faulting instruction ===================== ===================== = 0: 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax 6: 73 01 jae 0x9 8: c3 ret 9: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c19 10: f7 d8 neg %eax 12: 64 89 01 mov %eax,%fs:(%rcx) 15: 48 rex.W		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 0000000000000031 RAX: ffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7 RDX: 000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 0000000000000005 RBP: 0000000000000005 R08: 1999999999999999 R09: 0000000000000000 R10: 00007f59b9253298 R11: 000000000000 ---truncated--- **CVE ID : CVE-2024-53139**		
Out-of-bounds Read	02-Dec-2024	7.1	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adjust VSDB parser for replay feature At some point, the IEEE ID identification for the replay check in the AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN: [27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesy	https://git.kernel.org/stable/c/0a326fbc8f72a320051f27328d4d4e7abdfe68d7, https://git.kernel.org/stable/c/16dd2825c23530f2259fc671960a3a65d2af69bd, https://git.kernel.org/stable/c/8	O-LIN-LINU-241224/1471

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nc_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 ... [27.821207] Memory state around the buggy address: [27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821268] ==	db867061f4c76505ad62422b65d666b45289217	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is caused because the ID extraction happens outside of the range of the edid lenght. This commit addresses this issue by considering the amd_vsdb_block size. (cherry picked from commit b7e381b1ccd5e778e3d9c44c669ad38439a861d8) **CVE ID : CVE-2024-53108**		
N/A	04-Dec-2024	6.5	In the Linux kernel, the following vulnerability has been resolved: KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the implementation, some of which are fatal to the guest, and others which put the stability and health of the host at risk. For guest fatalities, the most glaring issue is that KVM fails to ensure	https://git.kernel.org/stable/c/aa0d42cacf093a6fcca872edc954f6f812926a17, https://git.kernel.org/stable/c/b91bb0ce5cd7005b376eac690ec664c1b56372ec, https://git.kernel.org/stable/c/d28b059ee4779b5102c5da6e929762520510e406	O-LIN-LINU-241224/1472

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tracing is disabled, and *stays* disabled prior to VM-Enter, which is necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing is enabled (enforced via a VMX consistency check). Per the SDM: If the logical processor is operating with Intel PT enabled (if IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load IA32_RTIT_CTL" VM-entry control must be 0. On the host side, KVM doesn't validate the guest CPUID configuration provided by userspace, and even worse, uses the guest configuration to decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring guest CPUID to enumerate more address ranges than are supported in hardware will result in KVM trying to passthrough, save, and load non-existent MSRs, which generates a variety of WARNs, ToPA ERRORs in the host, a potential deadlock, etc. **CVE ID : CVE-2024-53135**		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: prevent integer overflow in pagemap_scan_get_args() The "arg->vec_len" variable is a u64 that comes from the user at the start of the function. The "arg->vec_len * sizeof(struct page_region))" multiplication can lead to integer wrapping. Use size_mul() to avoid that. Also the size_add/mul() functions work on unsigned long so for 32bit systems we need to ensure that "arg->vec_len" fits in an unsigned long. **CVE ID : CVE-2024-53107**	https://git.kernel.org/stable/c/669b0cb81e4e7e8cff77a5b367c7f70c0c6c05e, https://git.kernel.org/stable/c/adee03f8903c58a6a559f21388a430211fac8ce9	O-LIN-LINU-241224/1473
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nommu: pass NULL argument to vma_iter_prealloc() When deleting a vma entry from a maple tree, it has to pass NULL to	https://git.kernel.org/stable/c/247d720b2c5d22f7281437fd6054a138256986ba, https://git.kernel.org/stable/c/8	O-LIN-LINU-241224/1474

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vma_iter_prealloc() in order to calculate internal state of the tree, but it passed a wrong argument. As a result, nommu kernels crashed upon accessing a vma iterator, such as acct_collect() reading the size of vma entries after do_munmap(). This commit fixes this issue by passing a right argument to the preallocation call. **CVE ID : CVE-2024-53109**	bbf0ab631cdf1dade6745f137cff98751e6ced7, https://git.kernel.org/stable/c/aceaf33b7666b72dfb86e0aa977be81e3bcbc727	
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. **CVE ID : CVE-2024-53110**	https://git.kernel.org/stable/c/0a886489d274596ad1a80789d3a773503210a615, https://git.kernel.org/stable/c/4e39ecadf1d2a08187139619f1f314b64ba7d947, https://git.kernel.org/stable/c/870d68fe	O-LIN-LINU-241224/1475

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				17b5d9032049dcad98b5781a344a8657	
Integer Overflow or Wraparound	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix address wraparound in move_page_tables() On 32-bit platforms, it is possible for the expression `len + old_addr < old_end` to be false-positive if `len + old_addr` wraps around. `old_addr` is the cursor in the old range up to which page table entries have been moved; so if the operation succeeded, `old_addr` is the *end* of the old region, and adding `len` to it can wrap. The overflow causes mremap() to mistakenly believe that PTEs have been copied; the consequence is that mremap() bails out, but doesn't move the PTEs back before the new VMA is unmapped, causing anonymous pages in the	https://git.kernel.org/stable/c/909543dc279a91122fb08e4653a72b82f0ad28f4, https://git.kernel.org/stable/c/a4a282daf1a190f03790bf163458ea3c8d28d217	O-LIN-LINU-241224/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			region to be lost. So basically if userspace tries to mremap() a
			private-anon region and hits this bug, mremap() will return an error and
			the private-anon region's contents appear to have been zeroed.
			
			The idea of this check is that `old_end - len` is the original start
			address, and writing the check that way also makes it easier to read; so
			fix the check by rearranging the comparison accordingly.
			
			(An alternate fix would be to refactor this function by introducing an
			"orig_old_start" variable or such.)
			
			Tested in a VM with a 32-bit X86 kernel; without the patch:
			```
			user@horn:~/big_mremap$ cat test.c
			#define _GNU_SOURCE
			#include <stdlib.h>
			#include <stdio.h>
			#include <err.h>
			```

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			#include <sys/mman.h>
			
			#define ADDR1 ((void*)0x60000000)
			#define ADDR2 ((void*)0x10000000)
			#define SIZE 0x50000000uL
			
			int main(void) {
			unsigned char *p1 = mmap(ADDR1, SIZE, PROT_READ|PROT_WRITE,
			MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED_NOREPLACE, -1, 0);
			if (p1 == MAP_FAILED)
			err(1, "mmap 1");
			unsigned char *p2 = mmap(ADDR2, SIZE, PROT_NONE,
			MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED_NOREPLACE, -1, 0);
			if (p2 == MAP_FAILED)
			err(1, "mmap 2");
			*p1 = 0x41;
			printf("first char is 0x%02hhx\n", *p1);
			unsigned char *p3 = mremap(p1, SIZE, SIZE,
			MREMAP_MAYMOVE|MREMAP_FIXED, p2);
			if (p3 == MAP_FAILED) {		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			printf("mremap() failed; first char is 0x%02hhx\n", *p1);
			} else {
			printf("mremap() succeeded; first char is 0x%02hhx\n", *p3);
			}
			}
			user@horn:~/big_mremap$ gcc -static -o test test.c
			user@horn:~/big_mremap$ setarch -R ./test
			first char is 0x41
			mremap() failed; first char is 0x00
			```
			With the patch:
			```
			user@horn:~/big_mremap$ setarch -R ./test
			first char is 0x41
			mremap() succeeded; first char is 0x41
			```
			CVE ID : CVE-2024-53111
			```

N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group	https://git.kernel.org/stable/c/620d22598110b0d0cb97a3fcca65fc473ea86e73,	O-LIN-LINU-241224/1477

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? do_error_trap+0x1dc/0x2c0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10 ? handle_invalid_op+0x34/0x40 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160	https://git.kernel.org/stable/c/737f34137844d6572ab7d473c998c7f977ff30eb, https://git.kernel.org/stable/c/843dfc804af4b338ead42331dd58081b428ecdf8	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10 ? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0 ? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160 ? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780 ? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... </TASK> When 'ioctl(OCFS2_IOC_GROUP_ADD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'. **CVE ID : CVE-2024-53112**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets. When cpuset is enabled, in prepare_alloc_pages(), ac->nodemask may be &current->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac->nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node,	https://git.kernel.org/stable/c/31502374627ba9ec3e710dbd0bb00457cc6d2c19, https://git.kernel.org/stable/c/6addb2d9501ec866d7b3a3b4e665307c437e9be2, https://git.kernel.org/stable/c/8ce41b0f9d77cca074df25afd39b86e2ee3aa68e	O-LIN-LINU-241224/1478

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when traversing Node1 in ac->zonelist, the nodemask is 2, and when traversing Node2 in ac->zonelist, the nodemask is 1. As a result, the ac->preferred_zoneref points to NULL zone. In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nodemask() finds a allowable zone and calls zonelist_node_idx(ac.preferred_zoneref), leading to NULL pointer dereference. __alloc_pages_noprof() fixes this issue by checking NULL pointer in commit ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath"). To fix it, check NULL pointer for preferred_zoneref->zone. **CVE ID : CVE-2024-53113**		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0	O-LIN-LINU-241224/1479

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			x86/CPU/AMD: Clear virtualized VMLOAD/VMSAVE on Zen4 client A number of Zen4 client SoCs advertise the ability to use virtualized VMLOAD/VMSAVE, but using these instructions is reported to be a cause of a random host reboot. These instructions aren't intended to be advertised on Zen4 client so clear the capability. **CVE ID : CVE-2024-53114**	0c713f84f477a85e524f34aad8fbd11a1c051f0, https://git.kernel.org/stable/c/a5ca1dc46a6b610dd4627d8b633d6c84f9724ef0	
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: avoid null_ptr_deref in vmw_framebuffer_surface_create_handle The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_create_handle.	https://git.kernel.org/stable/c/36f64da080555175b58d85f99f5f90435e274e56, https://git.kernel.org/stable/c/93d1f41a82de382845af460bf03bcb17dcbf08c5	O-LIN-LINU-241224/1480

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-53115		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix handling of partial GPU mapping of BOs This commit fixes the bug in the handling of partial mapping of the buffer objects to the GPU, which caused kernel warnings. Panthor didn't correctly handle the case where the partial mapping spanned multiple scatterlists and the mapping offset didn't point to the 1st page of starting scatterlist. The offset variable was not cleared after reaching the starting scatterlist. Following warning messages were seen. WARNING: CPU: 1 PID: 650 at drivers/iommu/io-pgtable-arm.c:659 __arm_lpae_unmap+0x254/0x5a0 <snip>	https://git.kernel.org/stable/c/3387e043918e154ca08d83954966a8b087fe2835, https://git.kernel.org/stable/c/d3e61af64b770e0038470c81f42bd1d0598f6bcc	O-LIN-LINU-241224/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pc : __arm_lpae_unmap+0x254/0x5a0 lr : __arm_lpae_unmap+0x2cc/0x5a0 <snip> Call trace: __arm_lpae_unmap+0x254/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 arm_lpae_unmap_pages+0x80/0xa0 panthor_vm_unmap_pages+0xac/0x1c8 [panthor] panthor_gpuva_sm_step_unmap+0x4c/0xc8 [panthor] op_unmap_cb.isra.23.constprop.30+0x54/0x80 __drm_gpuvm_sm_unmap+0x184/0x1c8 drm_gpuvm_sm_unmap+0x40/0x60		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			panthor_vm_exec_op+0xa8/0x120 [panthor] panthor_vm_bind_exec_sync_op+0xc4/0xe8 [panthor] panthor_ioctl_vm_bind+0x10c/0x170 [panthor] drm_ioctl_kernel+0xbc/0x138 drm_ioctl+0x210/0x4b0 __arm64_sys_ioctl+0xb0/0xf8 invoke_syscall+0x4c/0x110 el0_svc_common.constprop.1+0x98/0xf8 do_el0_svc+0x24/0x38 el0_svc+0x34/0xc8 el0t_64_sync_handler+0xa0/0xc8 el0t_64_sync+0x174/0x178 <snip> panthor : [drm] drm_WARN_ON(unmapped_sz != pgsize * pgcount) WARNING: CPU: 1 PID: 650 at drivers/gpu/drm/panthor/panthor_mmu.c:922 panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pc : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] lr : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip> panthor : [drm] *ERROR* failed to unmap range ffffa388f000-ffffa3890000 (requested range ffffa388c000-ffffa3890000) **CVE ID : CVE-2024-53116**		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Improve MSG_ZEROCOPY error handling Add a missing kfree_skb() to prevent memory leaks. **CVE ID : CVE-2024-53117**	https://git.kernel.org/stable/c/50061d7319e21165d04e3024354c1b43b6137821, https://git.kernel.org/stable/c/60cf6206a1f513512f5d73fa4d3dbbcad2e7dcd6	O-LIN-LINU-241224/1482
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix sk_error_queue memory leak	https://git.kernel.org/stable/c/bea4779a45f49275b1e1b1bd9de03cd37272	O-LIN-LINU-241224/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Kernel queues MSG_ZEROCOPY completion notifications on the error queue. Where they remain, until explicitly recv()ed. To prevent memory leaks, clean up the queue when the socket is destroyed. unreferenced object 0xffff8881028beb00 (size 224): comm "vsock_test", pid 1218, jiffies 4294694897 hex dump (first 32 bytes): 90 b0 21 17 81 88 ff ff 90 b0 21 17 81 88 ff ff ..!.......!..... 00 00 00 00 00 00 00 00 00 b0 21 17 81 88 ff ff ....!..... backtrace (crc 6c7031ca): [<ffffffff81418ef7>] kmem_cache_alloc_node_noprof+0x2f7/0x370 [<ffffffff81d35882>] __alloc_skb+0x132/0x180 [<ffffffff81d2d32b>] sock_omalloc+0x4b/0x80 [<ffffffff81d3a8ae>] msg_zerocopy_realloc+0x9e/0x240 [<ffffffff81fe5cb2>] virtio_transport_send_pkt_info+0x412/0x4c0 [<ffffffff81fe6183>] virtio_transport_stream_enqueue+0x43/0x50	44d8, https://git.kernel.org/stable/c/fbf7085b3ad1c7cc0677834c90f985f1b4f77a33	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff81fe0813>] vsock_connectible_sendmsg+0x373/0x450 [<ffffffff81d233d5>] ____sys_sendmsg+0x365/0x3a0 [<ffffffff81d246f4>] ___sys_sendmsg+0x84/0xd0 [<ffffffff81d26f47>] __sys_sendmsg+0x47/0x80 [<ffffffff820d3df3>] do_syscall_64+0x93/0x180 [<ffffffff8220012b>] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID : CVE-2024-53118**		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Fix accept_queue memory leak As the final stages of socket destruction may be delayed, it is possible that virtio_transport_recv_listen() will be called after the accept_queue has been flushed, but before the SOCK_DONE flag has been set. As a result, sockets enqueued after the flush would remain unremoved, leading to a memory leak.	https://git.kernel.org/stable/c/2415345042245de7601dcc6eafdbe3a3dcc9e379, https://git.kernel.org/stable/c/897617a413e0bf1c6380e3b34b2f28f450508549, https://git.kernel.org/stable/c/946c7600fa2207c	O-LIN-LINU-241224/1484

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_release __vsock_release lock virtio_transport_release virtio_transport_close schedule_delayed_work(close_work) sk_shutdown = SHUTDOWN_MASK (!) flush accept_queue release virtio_transport_recv_pkt vsock_find_bound_socket lock if flag(SOCK_DONE) return virtio_transport_recv_listen child = vsock_create_connected (!) vsock_enqueue_accept(child) release close_work lock virtio_transport_do_close set_flag(SOCK_DONE) virtio_transport_remove_sock vsock_remove_sock	c8d3fbc86a518ec56f98a5813	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_remove_bound release Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction. unreferenced object 0xffff888109e3f800 (size 2040): comm "kworker/5:2", pid 371, jiffies 4294940105 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 (..@............ backtrace (crc 9e5f4e84): [<ffffffff81418ff1>] kmem_cache_alloc_noprof+0x2c1/0x360 [<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120 [<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0 [<ffffffff81fe049a>] __vsock_create.constprop.0+0x2a/0x310 [<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0x4dc/0x9a0 [<ffffffff81fe745d>] vsock_loopback_work+0xfd/0x140		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff810fc6ac>] process_one_work+0x20c/0x570 [<ffffffff810fce3f>] worker_thread+0x1bf/0x3a0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<ffffffff81044fdd>] ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0x30 **CVE ID : CVE-2024-53119**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr-deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule(), in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000110 RIP: 0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core]	https://git.kernel.org/stable/c/06dc488a593020bd2f006798557d2a32104d8359, https://git.kernel.org/stable/c/0c7c70ff8b696cfedba350411dca736361ef9a0f, https://git.kernel.org/stable/c/6030f8bd7902e9e276a0edc09bf11	O-LIN-LINU-241224/1485

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0x30 ? mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] ? mlx5_tc_ct_entry_add_rule+0x1d5/0x2f0 [mlx5_core] mlx5_tc_ct_block_flow_offload+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] flow_offload_work_handler+0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x15b/0x2b0 process_one_work+0x16c/0x320	979e4e2bc2e	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker_thread+0x28c/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xb8/0xf0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> **CVE ID : CVE-2024-53120**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray.	https://git.kernel.org/stable/c/094d1a2121cee1e85ab07d74388f94809dcfb5b9, https://git.kernel.org/stable/c/933ef0d17f012b653e9e6006e3f50c8d0238b5ed, https://git.kernel.org/stable/c/9c	O-LIN-LINU-241224/1486

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely, causing a panic during subsequent rule deletions. To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to an FTE that is in the process of deletion. [438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func [438.968205] ------------[cut here]------------ [438.968654] refcount_t: decrement hit 0; leaking memory. [438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xfb/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch	a314419930f9135727e39d77e66262d5f7bef6	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower] [438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [438.974874] RIP: 0010:refcount_warn_saturate+0xfb/0x110 [438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90 [438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286 [438.977446] RAX: 0000000000000000 RBX:		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff888119d56de0 RCX: 0000000000000000 [438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0 [438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0 [438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0 [438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0 [438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:0000000000000000 [438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 0000000000372eb0 [438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [438.985842] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [438.986507] Call Trace: [438.986799] <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.987070] ? __warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xfb/0x110 [438.987877] ? report_bug+0x17d/0x190 [438.988261] ? prb_read_valid+0x17/0x20 [438.988659] ? handle_bug+0x53/0x90 [438.989054] ? exc_invalid_op+0x14/0x70 [438.989458] ? asm_exc_invalid_op+0x16/0x20 [438.989883] ? refcount_warn_saturate+0xfb/0x110 [438.990348] mlx5_del_flow_rules+0x2f7/0x340 [mlx5_core] [438.990932] __mlx5_eswitch_del_rule+0x49/0x170 [mlx5_core] [438.991519] ? mlx5_lag_is_sriov+0x3c/0x50 [mlx5_core] [438.992054] ? xas_load+0x9/0xb0 [438.992407] mlx5e_tc_rule_unoffload+0x45/0xe0 [mlx5_core] [438.993037] mlx5e_tc_del_fdb_flow+0x2a6/0x2e0 [mlx5_core] [438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261/0x390 [mlx5_core] [438.994728] tc_setup_cb_destroy+0xb9/0x190 [438.995150] fl_hw_destroy_filter+0x94/0xc0 [cls_flower] [438.995650] fl_change+0x11a4/0x13c0 [cls_flower] [438.996105] tc_new_tfilter+0x347/0xbc0 [438.996503] ? __ ---truncated--- **CVE ID : CVE-2024-53121**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: cope racing subflow creation in mptcp_rcv_space_adjust Additional active subflows - i.e. created by the in kernel path manager - are included into the subflow list before starting the 3whs. A racing recvmsg() spooling data received on an already established subflow would unconditionally call	https://git.kernel.org/stable/c/24995851d58c4a205ad0ffa7b2f21e479a9c8527, https://git.kernel.org/stable/c/aad6412c63baa39dd813e81f16a14d976b3de2e8, https://git.kernel.org/stable/c/ce	O-LIN-LINU-241224/1487

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). **CVE ID : CVE-2024-53122**	7356ae35943cc6494cc692e62d51a734062b7d	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024	https://git.kernel.org/stable/c/581302298524e9d77c4c44ff5156a6cd112227ae, https://git.kernel.org/stable/c/955388e1d5d222c4101c596b536d41b91a8b212e, https://git.kernel.org/stable/c/a66805c9b22caf4e42af7a616f6c6b	O-LIN-LINU-241224/1488

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:__tcp_select_window+ 0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80 R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033	83c90d1 010	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289 inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline] __se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559 RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef and provided a nice reproducer.		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss. Catch the error and return without performing any additional operations on the current socket. **CVE ID : CVE-2024-53123**		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix "Missing outer runtime PM protection" warning Fix the following drm_WARN: [953.586396] xe 0000:00:02.0: [drm] Missing outer runtime PM protection ... <4> [953.587090] ? xe_pm_runtime_get_noresume+0x8d/0xa0 [xe] <4> [953.587208] guc_exec_queue_add_msg+0x28/0x130 [xe]	https://git.kernel.org/stable/c/c0403e4ceecaefbeaf78263dffcd3e3f06a19f6b, https://git.kernel.org/stable/c/ed7cd3510d8da6e3578d9125a9ea4440f8adeeaa	O-LIN-LINU-241224/1489

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<4> [953.587319] guc_exec_queue_fini+0x3a/0x40 [xe] <4> [953.587425] xe_exec_queue_destroy+0xb3/0xf0 [xe] <4> [953.587515] xe_oa_release+0x9c/0xc0 [xe] (cherry picked from commit b107c63d2953907908fd0cafb0e543b3c3167b75) **CVE ID : CVE-2024-53132**		
Always-Incorrect Control Flow Implementation	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: correct remove path The check condition should be 'i < bc->onecell_data.num_domains', not 'bc->onecell_data.num_domains' which will make the look never finish and cause kernel panic. Also disable runtime to address "imx93-blk-ctrl 4ac10000.system-controller: Unbalanced pm_runtime_enable!" **CVE ID : CVE-2024-53134**	https://git.kernel.org/stable/c/201fb9e164a1e4c5937de2cf58bcb0327c08664f, https://git.kernel.org/stable/c/8fc228ab5d38a026eae7183a5f74a4fac43d9b6a, https://git.kernel.org/stable/c/f7c7c5aa556378a2c8da72c1f7f238	O-LIN-LINU-241224/1490

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b6648f95fb	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ARM: fix cacheflush with PAN It seems that the cacheflush syscall got broken when PAN for LPAE was implemented. User access was not enabled around the cache maintenance instructions, causing them to fault. **CVE ID : CVE-2024-53137**	https://git.kernel.org/stable/c/ca29cfcc4a21083d671522ad384532e28a43f033, https://git.kernel.org/stable/c/e6960a2ed49c9a25357817535f7cc50594a58604	O-LIN-LINU-241224/1491
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resync_dump_comp()), only put_page() is used.	https://git.kernel.org/stable/c/2723e8b2cbd486cb96e5a61b22473f7fd62e18df, https://git.kernel.org/stable/c/69fbd07f17b0fdaf8970bc705f5bf115c297839d, https://	O-LIN-LINU-241224/1492

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 is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc() references are stored directly in the given page. On release the folio page will be dereferenced too many times. This was found while doing kTLS testing with sendfile() + ZC when the served file was read from NFS on a kernel with NFS large folios support (commit 49b29a573da8 ("nfs: add support for large folios")). **CVE ID : CVE-2024-53138**	git.kernel.org/stable/c/93a14620b97c911489a5b008782f3d9b0c4aeff4	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: net: fix data-races around sk->sk_forward_alloc Syzkaller reported this warning: ------------[cut here]------------ WARNING: CPU: 0 PID: 16 at net/ipv4/af_inet.c:156 inet_sock_destruct+0x1c5/0x1e0 Modules linked in:	https://git.kernel.org/stable/c/073d89808c065ac4c672c0a613a71b27a80691cb, https://git.kernel.org/stable/c/d285eb9d0641c8344f2836081b4cc	O-LIN-LINU-241224/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.12.0-rc5 #26 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:inet_sock_destruct+0x1c5/0x1e0 Code: 24 12 4c 89 e2 5b 48 c7 c7 98 ec bb 82 41 5c e9 d1 18 17 ff 4c 89 e6 5b 48 c7 c7 d0 ec bb 82 41 5c e9 bf 18 17 ff 0f 0b eb 83 <0f> 0b eb 97 0f 0b eb 87 0f 0b e9 68 ff ff ff 66 66 2e 0f 1f 84 00 RSP: 0018:ffffc9000008bd90 EFLAGS: 00010206 RAX: 0000000000000300 RBX: ffff88810b172a90 RCX: 0000000000000007 RDX: 0000000000000002 RSI: 0000000000000300 RDI: ffff88810b172a00 RBP: ffff88810b172a00 R08: ffff888104273c00 R09: 0000000000100007 R10: 0000000000020000 R11: 0000000000000006 R12: ffff88810b172a00 R13: 0000000000000004 R14: 0000000000000000 R15: ffff888237c31f78 FS: 0000000000000000(0000) GS:ffff888237c00000(0000) knlGS:0000000000000000	b7b3c5c c1b6	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffc63fecac8 CR3: 000000000342e000 CR4: 00000000000006f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __warn+0x88/0x130 ? inet_sock_destruct+0x1c5/0x1e0 ? report_bug+0x18e/0x1a0 ? handle_bug+0x53/0x90 ? exc_invalid_op+0x18/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? inet_sock_destruct+0x1c5/0x1e0 __sk_destruct+0x2a/0x200 rcu_do_batch+0x1aa/0x530 ? rcu_do_batch+0x13b/0x530 rcu_core+0x159/0x2f0 handle_softirqs+0xd3/0x2b0		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_smpboot_thread_fn+0x10/0x10 run_ksoftirqd+0x25/0x30 smpboot_thread_fn+0xdd/0x1d0 kthread+0xd3/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- Its possible that two threads call tcp_v6_do_rcv()/sk_forward_alloc_add() concurrently when sk->sk_state == TCP_LISTEN with sk->sk_lock unlocked, which triggers a data-race around sk->sk_forward_alloc: tcp_v6_rcv tcp_v6_do_rcv skb_clone_and_charge_r sk_rmem_schedule __sk_mem_schedule sk_forward_alloc_add()		

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

*stands for all versions

<table>
<tr><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></tr>
<tr><td></td><td></td><td></td><td>skb_set_owner_r
sk_mem_charge
sk_forward_alloc_add()
__kfree_skb
skb_release_all
skb_release_head_state
sock_rfree
sk_mem_uncharge
sk_forward_alloc_add()
sk_mem_reclaim
// set local var reclaimable
__sk_mem_reclaim
sk_forward_alloc_add()
In this syzkaller testcase, two threads call
tcp_v6_do_rcv() with skb->truesize=768, the sk_forward_alloc changes like
this:
(cpu 1) | (cpu 2) | sk_forward_alloc
... | ... | 0
__sk_mem_schedule() | | +4096 = 4096
| __sk_mem_schedule() | +4096 = 8192</td><td></td><td></td></tr>
</table>

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sk_mem_charge() | | -768 = 7424 | sk_mem_charge() | -768 = 6656 ... | ... | sk_mem_uncharge() | | +768 = 7424 reclaimable=7424 | | | sk_mem_uncharge() | +768 = 8192 | reclaimable=8192 | __sk_mem_reclaim() | | -4096 = 4096 | __sk_mem_reclaim() | -8192 = -4096 != 0 The skb_clone_and_charge_r() should not be called in tcp_v6_do_rcv() when sk->sk_state is TCP_LISTEN, it happens later in tcp_v6_syn_recv_sock(). Fix the same issue in dccp_v6_do_rcv(). **CVE ID : CVE-2024-53124**		
Affected Version(s): From (including) 2.6.12 Up to (excluding) 4.19.325					
Out-of-bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun	https://git.kernel.org/stable/c/1a423bbbeaf9e3e20c46865	O-LIN-LINU-241224/1494

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 initramfs filename field is defined in Documentation/driver-api/early-userspace/buffer-format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data ... 55 ============= ================== ===================== ==== 56 Field name Field size Meaning 57 ============= ================== ===================== ==== ... 70 c_namesize 8 bytes Length of filename, including final \0 When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero-terminated path at @collected, passing it directly to filp_open() / init_mkdir() / init_mknod(). If a specially crafted cpio entry carries a non-zero-terminated filename	01efd9b661fe834db, https://git.kernel.org/stable/c/49d01e736c3045319e030d1e75fb983011abaca7, https://git.kernel.org/stable/c/bb7ac96670ab1d8d681015f9d66e45dad579af4d	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is followed by uninitialized memory, then a file may be created with trailing characters that represent the uninitialized memory. The ability to create an initramfs entry would imply already having full control of the system, so the buffer overrun shouldn't be considered a security vulnerability.
			Append the output of the following bash script to an existing initramfs and observe any created /initramfs_test_fname_overrunAA* path. E.g.
			./reproducer.sh | gzip >> /myinitramfs
			It's easiest to observe non-zero uninitialized memory when the output is gzipped, as it'll overflow the heap allocated @out_buf in __gunzip(), rather than the initrd_start+initrd_size block.
			---- reproducer.sh ----
			nilchar="A" # change to "\0" to properly zero terminate / pad
			magic="070701"		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ino=1 mode=$((0100777)) uid=0 gid=0 nlink=1 mtime=1 filesize=0 devmajor=0 devminor=1 rdevmajor=0 rdevminor=0 csum=0 fname="initramfs_test_fname_overrun" namelen=$((${#fname} + 1)) # plus one to account for terminator printf "%s%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%s" \\ $magic $ino $mode $uid $gid $nlink $mtime $filesize \\ $devmajor $devminor $rdevmajor $rdevminor $namelen $csum $fname termpadlen=$((1 + ((4 - ((110 + $namelen) & 3)) % 4))) printf "%.s${nilchar}" $(seq 1 $termpadlen) ---- reproducer.sh ----		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Symlink filename fields handled in do_symlink() won't overrun past the data segment, due to the explicit zero-termination of the symlink target. Fix filename buffer overrun by aborting the initramfs FSM if any cpio entry doesn't carry a zero-terminator at the expected (name_len - 1) offset. **CVE ID : CVE-2024-53142**		
Affected Version(s): From (including) 2.6.25 Up to (excluding) 4.19.325					
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0	https://git.kernel.org/stable/c/620d22598110b0d0cb97a3fcca65fc473ea86e73, https://git.kernel.org/stable/c/737f34137844d6572ab7d473c998c7f977ff30eb, https://git.kernel.org/sta	O-LIN-LINU-241224/1495

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? do_error_trap+0x1dc/0x2c0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10 ? handle_invalid_op+0x34/0x40 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160 ? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10	ble/c/843dfc804af4b338ead42331dd58081b428ecdf8	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0 ? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160 ? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0 ? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... </TASK> When 'ioctl(OCFS2_IOC_GROUP_ADD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'. **CVE ID : CVE-2024-53112**		
Affected Version(s): From (including) 2.6.39 Up to (excluding) 4.19.325					

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE ID : CVE-2024-53141**	https://git.kernel.org/stable/c/15794835378ed56fb9bacc6a5dd3b9f33520604e, https://git.kernel.org/stable/c/35f56c554eb1b56b77b3cf197a6b00922d49033d, https://git.kernel.org/stable/c/3c20b5948f119ae61ee35ad8584d666020c91581	O-LIN-LINU-241224/1496
Affected Version(s): From (including) 3.9 Up to (excluding) 6.1.119					
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer"	https://git.kernel.org/stable/c/2026559a6c4ce34db117d2db8f710fe2a9420d5a, https://git.kerne	O-LIN-LINU-241224/1497

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	tracepoint, mark_buffer_dirty() may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b-tree node blocks, does not set the block device, but instead does so only if the buffer is not in the "uptodate" state for each of its caller block reading functions. However, if the uptodate flag is set on a folio/page, and the buffer heads are detached from it by try_to_free_buffers(), and new buffer	l.org/stable/c/7af3309c7a2ef26831a67125b11c34a7e01c1b2a, https://git.kernel.org/stable/c/86b19031dbc79abc378dfae357f6ea33ebeb0c95	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heads are then attached by create_empty_buffers(), the uptodate flag may be restored to each buffer without the block device being set to bh->b_bdev, and mark_buffer_dirty() may be called later in that state, resulting in the bug mentioned above. Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag. **CVE ID : CVE-2024-53130**		
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint Patch series "nilfs2: fix null-ptr-deref bugs on block tracepoints". This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints.	https://git.kernel.org/stable/c/085556bf8c70e2629e02e79268dac3016a08b8bf, https://git.kernel.org/stable/c/3b2a4fd9bbee77afdd3ed5a05a0c02b6cde8d3b9, https://	O-LIN-LINU-241224/1498

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
			This patch (of 2): It has been reported that when using "block:block_touch_buffer" tracepoint, touch_buffer() called from __nilfs_get_folio_block() causes a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because since the tracepoint was added in touch_buffer(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, the block_device structure is set after the function returns to the caller. Here, touch_buffer() is used to mark the folio/page that owns the buffer head as accessed, but the common search helper for folio/page used by the caller function was optimized to mark the	git.kernel.org/stable/c/59b49ca67cca7b007a5afd3de0283c8008157665	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			folio/page as accessed when it was reimplemented a long time ago, eliminating the need to call touch_buffer() here in the first place. So this solves the issue by eliminating the touch_buffer() call itself. **CVE ID : CVE-2024-53131**		
Affected Version(s): From (including) 4.19.322 Up to (excluding) 4.20					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K" The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110	https://git.kernel.org/stable/c/00bff71745bc3583bd5ca59be91e0ee1d27f1944, https://git.kernel.org/stable/c/1635e407a4a64d08a8517ac59ca14ad4fc785e75, https://git.kernel.org/stable/c/56de724c58c07a7ca3aac027cfd2c	O-LIN-LINU-241224/1499

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe0891080f8cab7890. **CVE ID : CVE-2024-53127**	cb184ed9e4e	
Affected Version(s): From (including) 4.19.323 Up to (excluding) 4.19.325					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kernel.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	O-LIN-LINU-241224/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 4.20 Up to (excluding) 6.1.119					
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? do_error_trap+0x1dc/0x2c0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10 ? handle_invalid_op+0x34/0x40	https://git.kernel.org/stable/c/620d22598110b0d0cb97a3fcca65fc473ea86e73, https://git.kernel.org/stable/c/737f34137844d6572ab7d473c998c7f977ff30eb, https://git.kernel.org/stable/c/843dfc804af4b338ead42331dd58081b428ecdf8	O-LIN-LINU-241224/1501

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160 ? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10 ? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0 ? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160 ? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0 ? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780 ? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... </TASK> When 'ioctl(OCFS2_IOC_GROUP_A		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'. **CVE ID : CVE-2024-53112**		
Affected Version(s): From (including) 4.20 Up to (excluding) 6.6.64					
N/A	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check	https://git.kernel.org/stable/c/15794835378ed56fb9bacc6a5dd3b9f33520604e, https://git.kernel.org/stable/c/35f56c554eb1b56b77b3cf197a6b00922d49033d,	O-LIN-LINU-241224/1502

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE ID : CVE-2024-53141**	https://git.kernel.org/stable/c/3c20b5948f119ae61ee35ad8584d666020c91581	
Out-of-bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in Documentation/driver-api/early-userspace/buffer-format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data ... 55 ============= ================== ===================== ==== 56 Field name Field size Meaning 57 ============= ================== ===================== ==== ...	https://git.kernel.org/stable/c/1a423bbbeaf9e3e20c4686501efd9b661fe834db, https://git.kernel.org/stable/c/49d01e736c3045319e030d1e75fb983011abaca7, https://git.kernel.org/stable/c/bb7ac96670ab1d8d681015f9d66e45dad579af4d	O-LIN-LINU-241224/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			70 c_namesize 8 bytes Length of filename, including final \0 When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero-terminated path at @collected, passing it directly to filp_open() / init_mkdir() / init_mknod(). If a specially crafted cpio entry carries a non-zero-terminated filename and is followed by uninitialized memory, then a file may be created with trailing characters that represent the uninitialized memory. The ability to create an initramfs entry would imply already having full control of the system, so the buffer overrun shouldn't be considered a security vulnerability. Append the output of the following bash script to an existing initramfs and observe any created /initramfs_test_fname_overrunAA* path. E.g. ./reproducer.sh | gzip >> /myinitramfs		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			It's easiest to observe non-zero uninitialized memory when the output is
			gzipped, as it'll overflow the heap allocated @out_buf in __gunzip(),
			rather than the initrd_start+initrd_size block.
			
			---- reproducer.sh ----
			nilchar="A" # change to "\0" to properly zero terminate / pad
			magic="070701"
			ino=1
			mode=$((0100777))
			uid=0
			gid=0
			nlink=1
			mtime=1
			filesize=0
			devmajor=0
			devminor=1
			rdevmajor=0
			rdevminor=0
			csum=0
			fname="initramfs_test_fname_overrun"
			namelen=$((${#fname} + 1)) # plus one to account for terminator
			
			printf "%s%08x%08x%08x%08x		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			%08x%08x%08x%08x%08x%08x%08x%08x%08x%s" \ $magic $ino $mode $uid $gid $nlink $mtime $filesize \ $devmajor $devminor $rdevmajor $rdevminor $namelen $csum $fname termpadlen=$((1 + ((4 - ((110 + $namelen) & 3)) % 4))) printf "%.s${nilchar}" $(seq 1 $termpadlen) ---- reproducer.sh ---- Symlink filename fields handled in do_symlink() won't overrun past the data segment, due to the explicit zero-termination of the symlink target. Fix filename buffer overrun by aborting the initramfs FSM if any cpio entry doesn't carry a zero-terminator at the expected (name_len - 1) offset. **CVE ID : CVE-2024-53142**		
Affected Version(s): From (including) 4.4 Up to (excluding) 6.11.10					
Concurrent Execution using	02-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/sta	O-LIN-LINU-241224/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			net: fix data-races around sk->sk_forward_alloc Syzkaller reported this warning: ------------[cut here]------------ WARNING: CPU: 0 PID: 16 at net/ipv4/af_inet.c:156 inet_sock_destruct+0x1c5/0x1e0 Modules linked in: CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.12.0-rc5 #26 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:inet_sock_destruct+0x1c5/0x1e0 Code: 24 12 4c 89 e2 5b 48 c7 c7 98 ec bb 82 41 5c e9 d1 18 17 ff 4c 89 e6 5b 48 c7 c7 d0 ec bb 82 41 5c e9 bf 18 17 ff 0f 0b eb 83 <0f> 0b eb 97 0f 0b eb 87 0f 0b e9 68 ff ff ff 66 66 2e 0f 1f 84 00 RSP: 0018:ffffc9000008bd90 EFLAGS: 00010206 RAX: 0000000000000300 RBX: ffff88810b172a90 RCX: 0000000000000007	ble/c/073d89808c065ac4c672c0a613a71b27a80691cb, https://git.kernel.org/stable/c/d285eb9d0641c8344f2836081b4ccb7b3c5cc1b6	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000002 RSI: 0000000000000300 RDI: ffff88810b172a00 RBP: ffff88810b172a00 R08: ffff888104273c00 R09: 0000000000100007 R10: 0000000000020000 R11: 0000000000000006 R12: ffff88810b172a00 R13: 0000000000000004 R14: 0000000000000000 R15: ffff888237c31f78 FS: 0000000000000000(0000) GS:ffff888237c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffc63fecac8 CR3: 000000000342e000 CR4: 00000000000006f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __warn+0x88/0x130 ? inet_sock_destruct+0x1c5/0x1e0 ? report_bug+0x18e/0x1a0 ? handle_bug+0x53/0x90 ? exc_invalid_op+0x18/0x70		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? asm_exc_invalid_op+0x1a/0x20 ? inet_sock_destruct+0x1c5/0x1e0 __sk_destruct+0x2a/0x200 rcu_do_batch+0x1aa/0x530 ? rcu_do_batch+0x13b/0x530 rcu_core+0x159/0x2f0 handle_softirqs+0xd3/0x2b0 ? __pfx_smpboot_thread_fn+0x10/0x10 run_ksoftirqd+0x25/0x30 smpboot_thread_fn+0xdd/0x1d0 kthread+0xd3/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- Its possible that two threads call		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_v6_do_rcv()/sk_forward_alloc_add() concurrently when sk->sk_state == TCP_LISTEN with sk->sk_lock unlocked, which triggers a data-race around sk->sk_forward_alloc: tcp_v6_rcv tcp_v6_do_rcv skb_clone_and_charge_r sk_rmem_schedule __sk_mem_schedule sk_forward_alloc_add() skb_set_owner_r sk_mem_charge sk_forward_alloc_add() __kfree_skb skb_release_all skb_release_head_state sock_rfree sk_mem_uncharge sk_forward_alloc_add() sk_mem_reclaim // set local var reclaimable __sk_mem_reclaim sk_forward_alloc_add()		

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

*stands for all versions

<table>
<tr><th>Weakness</th><th>Publish Date</th><th>CVSSv3</th><th>Description &amp; CVE ID</th><th>Patch</th><th>NCIIPC ID</th></tr>
<tr><td></td><td></td><td></td><td>In this syzkaller testcase, two threads call
tcp_v6_do_rcv() with skb->truesize=768, the sk_forward_alloc changes like
this:
 (cpu 1) | (cpu 2) | sk_forward_alloc
 ... | ... | 0
 __sk_mem_schedule() | | +4096 = 4096
 | __sk_mem_schedule() | +4096 = 8192
 sk_mem_charge() | | -768 = 7424
 | sk_mem_charge() | -768 = 6656
 ... | ... |
 sk_mem_uncharge() | | +768 = 7424
 reclaimable=7424 | |
 | sk_mem_uncharge() | +768 = 8192
 | reclaimable=8192 |
 __sk_mem_reclaim() | | -4096 = 4096
 | __sk_mem_reclaim() | -8192 = -4096 != 0</td><td></td><td></td></tr>
</table>

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The skb_clone_and_charge_r() should not be called in tcp_v6_do_rcv() when sk->sk_state is TCP_LISTEN, it happens later in tcp_v6_syn_recv_sock(). Fix the same issue in dccp_v6_do_rcv(). **CVE ID : CVE-2024-53124**		
Affected Version(s): From (including) 4.4.38 Up to (excluding) 4.5					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered	https://git.kernel.org/stable/c/114a61d8d94ae3a43b82446cf737fd757021b834, https://git.kernel.org/stable/c/176c41b3ca9281a9736b67c6121b03dbf0c8c08f, https://git.kernel.org/stable/c/1904fb9ebf911441f90a68e96b22aa73e4410505	O-LIN-LINU-241224/1505

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in response to recvmsg() on the socket. This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone else holds the socket they may release it in BH and we're back to square one.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 whole dance, however, appears to be unnecessary. Only the user can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own. **CVE ID : CVE-2024-53140**		
Affected Version(s): From (including) 4.8.14 Up to (excluding) 4.9					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close	https://git.kernel.org/stable/c/114a61d8d94ae3a43b82446cf737fd757021b834, https://	O-LIN-LINU-241224/1506

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket. This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done	git.kernel.org/stable/c/176c41b3ca9281a9736b67c6121b03dbf0c8c08f, https://git.kernel.org/stable/c/1904fb9ebf911441f90a68e96b22aa73e4410505	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone else holds the socket they may release it in BH and we're back to square one. The whole dance, however, appears to be unnecessary. Only the user can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own. **CVE ID : CVE-2024-53140**		
Affected Version(s): From (including) 4.9 Up to (excluding) 6.1.119					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket.	https://git.kernel.org/stable/c/114a61d8d94ae3a43b82446cf737fd757021b834, https://git.kernel.org/stable/c/176c41b3ca9281a9736b67c6121b03dbf0c8c08f, https://git.kernel.org/stable/c/1904fb9ebf911441f90a68e96b22aa73e4410505	O-LIN-LINU-241224/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone else holds the socket they may release it in BH and we're back to square one.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 whole dance, however, appears to be unnecessary. Only the user can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own. **CVE ID : CVE-2024-53140**		
Affected Version(s): From (including) 5.0 Up to (excluding) 6.1.119					
N/A	04-Dec-2024	6.5	In the Linux kernel, the following vulnerability has been resolved: KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN	https://git.kernel.org/stable/c/aa0d42cacf093a6fcca872edc954f6f812926a17, https://	O-LIN-LINU-241224/1508

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the implementation, some of which are fatal to the guest, and others which put the stability and health of the host at risk. For guest fatalities, the most glaring issue is that KVM fails to ensure tracing is disabled, and *stays* disabled prior to VM-Enter, which is necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing is enabled (enforced via a VMX consistency check). Per the SDM: If the logical processor is operating with Intel PT enabled (if IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load IA32_RTIT_CTL" VM-entry control must be 0. On the host side, KVM doesn't validate the guest CPUID configuration	git.kernel.org/stable/c/b91bb0ce5cd7005b376eac690ec664c1b56372ec, https://git.kernel.org/stable/c/d28b059ee4779b5102c5da6e929762520510e406	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			provided by userspace, and even worse, uses the guest configuration to decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring guest CPUID to enumerate more address ranges than are supported in hardware will result in KVM trying to passthrough, save, and load non-existent MSRs, which generates a variety of WARNs, ToPA ERRORs in the host, a potential deadlock, etc. **CVE ID : CVE-2024-53135**		
Affected Version(s): From (including) 5.1 Up to (excluding) 6.1.119					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray.	https://git.kernel.org/stable/c/094d1a2121cee1e85ab07d74388f94809dcfb5b9, https://git.kernel.org/stable/c/933ef0d17f012b653e9e6006e3f50c8d0238b5ed, https://git.kernel.org/sta	O-LIN-LINU-241224/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely, causing a panic during subsequent rule deletions. To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to an FTE that is in the process of deletion. [438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func [438.968205] ------------[cut here]------------ [438.968654] refcount_t: decrement hit 0; leaking memory. [438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xfb/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch	ble/c/9ca314419930f9135727e39d77e66262d5f7bef6	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower] [438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [438.974874] RIP: 0010:refcount_warn_saturate+0xfb/0x110 [438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90 [438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286 [438.977446] RAX: 0000000000000000 RBX:		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff888119d56de0 RCX: 0000000000000000 [438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0 [438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0 [438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0 [438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0 [438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:0000000000000000 [438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 0000000000372eb0 [438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [438.985842] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [438.986507] Call Trace: [438.986799] <TASK>		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.987070] ? __warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xfb/0x110 [438.987877] ? report_bug+0x17d/0x190 [438.988261] ? prb_read_valid+0x17/0x20 [438.988659] ? handle_bug+0x53/0x90 [438.989054] ? exc_invalid_op+0x14/0x70 [438.989458] ? asm_exc_invalid_op+0x16/0x20 [438.989883] ? refcount_warn_saturate+0xfb/0x110 [438.990348] mlx5_del_flow_rules+0x2f7/0x340 [mlx5_core] [438.990932] __mlx5_eswitch_del_rule+0x49/0x170 [mlx5_core] [438.991519] ? mlx5_lag_is_sriov+0x3c/0x50 [mlx5_core] [438.992054] ? xas_load+0x9/0xb0 [438.992407] mlx5e_tc_rule_unoffload+0x45/0xe0 [mlx5_core] [438.993037] mlx5e_tc_del_fdb_flow+0x2a6/0x2e0 [mlx5_core] [438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261/0x390 [mlx5_core] [438.994728] tc_setup_cb_destroy+0xb9/0x190 [438.995150] fl_hw_destroy_filter+0x94/0xc0 [cls_flower] [438.995650] fl_change+0x11a4/0x13c0 [cls_flower] [438.996105] tc_new_tfilter+0x347/0xbc0 [438.996503] ? _ ---truncated--- **CVE ID : CVE-2024-53121**		
Affected Version(s): From (including) 5.10 Up to (excluding) 6.1.119					
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Fix accept_queue memory leak As the final stages of socket destruction may be delayed, it is possible that virtio_transport_recv_listen() will be called after the accept_queue has been flushed, but before the SOCK_DONE flag has been set. As a result, sockets enqueued after the flush would remain unremoved, leading to a	https://git.kernel.org/stable/c/2415345042245de7601dcc6eafdbe3a3dcc9e379, https://git.kernel.org/stable/c/897617a413e0bf1c6380e3b34b2f28f450508549, https://git.kernel.org/sta	O-LIN-LINU-241224/1510

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			memory leak. vsock_release __vsock_release lock virtio_transport_release virtio_transport_close schedule_delayed_work(close_work) sk_shutdown = SHUTDOWN_MASK (!) flush accept_queue release virtio_transport_recv_pkt vsock_find_bound_socket lock if flag(SOCK_DONE) return virtio_transport_recv_listen child = vsock_create_connected (!) vsock_enqueue_accept(child) release close_work lock virtio_transport_do_close set_flag(SOCK_DONE)	ble/c/946c7600fa2207cc8d3fbc86a518ec56f98a5813	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			virtio_transport_remove_sock vsock_remove_sock vsock_remove_bound release Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction. unreferenced object 0xffff888109e3f800 (size 2040): comm "kworker/5:2", pid 371, jiffies 4294940105 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 (..@............ backtrace (crc 9e5f4e84): [<ffffffff81418ff1>] kmem_cache_alloc_noprof+0x2c1/0x360 [<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120 [<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0 [<ffffffff81fe049a>] __vsock_create.constprop.0+0x2a/0x310		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0x4dc/0x9a0 [<ffffffff81fe745d>] vsock_loopback_work+0xfd/0x140 [<ffffffff810fc6ac>] process_one_work+0x20c/0x570 [<ffffffff810fce3f>] worker_thread+0x1bf/0x3a0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<ffffffff81044fdd>] ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0x30 **CVE ID : CVE-2024-53119**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: cope racing subflow creation in mptcp_rcv_space_adjust Additional active subflows - i.e. created by the in kernel path manager - are included into the subflow list before starting the 3whs.	https://git.kernel.org/stable/c/24995851d58c4a205ad0ffa7b2f21e479a9c8527, https://git.kernel.org/stable/c/aad6412c63baa39dd813e81f16a14d976b3de2e8, https://	O-LIN-LINU-241224/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			A racing recvmsg() spooling data received on an already established subflow would unconditionally call tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). **CVE ID : CVE-2024-53122**	git.kernel.org/stable/c/ce7356ae35943cc6494cc692e62d51a734062b7d	
Affected Version(s): From (including) 5.10.229 Up to (excluding) 5.11					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kernel.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kerne	O-LIN-LINU-241224/1512

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	l.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	
Affected Version(s): From (including) 5.13 Up to (excluding) 6.1.119					
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets. When cpuset is enabled, in prepare_alloc_pages(), ac->nodemask may be &current->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac->nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node,	https://git.kernel.org/stable/c/31502374627ba9ec3e710dbd0bb00457cc6d2c19, https://git.kernel.org/stable/c/6addb2d9501ec866d7b3a3b4e665307c437e9be2, https://git.kernel.org/stable/c/8ce41b0f9d77cca074df25afd39b86e2ee3aa68e	O-LIN-LINU-241224/1513

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when traversing Node1 in ac->zonelist, the nodemask is 2, and when traversing Node2 in ac->zonelist, the nodemask is 1. As a result, the ac->preferred_zoneref points to NULL zone. In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nodemask() finds a allowable zone and calls zonelist_node_idx(ac.preferred_zoneref), leading to NULL pointer dereference. __alloc_pages_noprof() fixes this issue by checking NULL pointer in commit ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath"). To fix it, check NULL pointer for preferred_zoneref->zone. **CVE ID : CVE-2024-53113**		
Affected Version(s): From (including) 5.14 Up to (excluding) 6.1.119					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr-deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule() , in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000110 RIP: 0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] … Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0x30	https://git.kernel.org/stable/c/06dc488a593020bd2f006798557d2a32104d8359, https://git.kernel.org/stable/c/0c7c70ff8b696cfedba350411dca736361ef9a0f, https://git.kernel.org/stable/c/6030f8bd7902e9e276a0edc09bf11979e4e2bc2e	O-LIN-LINU-241224/1514

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] ? mlx5_tc_ct_entry_add_rule+0x1d5/0x2f0 [mlx5_core] mlx5_tc_ct_block_flow_offload+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] flow_offload_work_handler+0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x15b/0x2b0 process_one_work+0x16c/0x320 worker_thread+0x28c/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xb8/0xf0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ret_from_fork_asm+0x1a/0x30 </TASK> **CVE ID : CVE-2024-53120**		
Affected Version(s): From (including) 5.15.171 Up to (excluding) 5.16					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kernel.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	O-LIN-LINU-241224/1515
Affected Version(s): From (including) 5.19 Up to (excluding) 6.1.119					
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0a886489	O-LIN-LINU-241224/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. **CVE ID : CVE-2024-53110**	d274596ad1a80789d3a773503210a615, https://git.kernel.org/stable/c/4e39ecadf1d2a08187139619f1f314b64ba7d947, https://git.kernel.org/stable/c/870d68fe17b5d9032049dcad98b5781a344a8657	
Affected Version(s): From (including) 5.4 Up to (excluding) 6.1.119					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release	https://git.kernel.org/stable/c/2723e8b2cbd486cb96e5a61b22473f7fd62e18df, https://git.kernel.org/stable/c/69fbd07f17b0fdaf8970bc	O-LIN-LINU-241224/1517

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			path (mlx5e_ktls_tx_handle_resync_dump_comp()), only put_page() is used. This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc() references are stored directly in the given page. On release the folio page will be dereferenced too many times. This was found while doing kTLS testing with sendfile() + ZC when the served file was read from NFS on a kernel with NFS large folios support (commit 49b29a573da8 ("nfs: add support for large folios")). **CVE ID : CVE-2024-53138**	705f5bf115c297839d, https://git.kernel.org/stable/c/93a14620b97c911489a5b008782f3d9b0c4aeff4	
Affected Version(s): From (including) 5.4.285 Up to (excluding) 5.5					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()"	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kerne	O-LIN-LINU-241224/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	l.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	
Affected Version(s): From (including) 6.1 Up to (excluding) 6.6.63					
Always-Incorrect Control Flow Implementation	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: correct remove path The check condition should be 'i < bc->onecell_data.num_domains', not 'bc->onecell_data.num_domains' which will make the look never finish and cause kernel panic. Also disable runtime to address "imx93-blk-ctrl 4ac10000.system-	https://git.kernel.org/stable/c/201fb9e164a1e4c5937de2cf58bcb0327c08664f, https://git.kernel.org/stable/c/8fc228ab5d38a026eae7183a5f74a4fac43d9b6a, https://git.kernel.org/stable/c/f7	O-LIN-LINU-241224/1519

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller: Unbalanced pm_runtime_enable!" **CVE ID : CVE-2024-53134**	c7c5aa556378a2c8da72c1f7f238b6648f95fb	
Affected Version(s): From (including) 6.1.0 Up to (excluding) 6.1.119					
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip/rockchip_drm_vop.c:1096 vop_plane_atomic_async_check() warn: variable dereferenced before check 'state' (see line 1077) **CVE ID : CVE-2024-53129**	https://git.kernel.org/stable/c/1e53059729691ca4d905118258b9fbd17d854174, https://git.kernel.org/stable/c/656dbd1c21c2c088c70059cdd43ec83e7d54ec4d, https://git.kernel.org/stable/c/ab1c793f457f740ab7108cc0b1340a402dbf484d	O-LIN-LINU-241224/1520
Affected Version(s): From (including) 6.1.110 Up to (excluding) 6.1.119					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0	O-LIN-LINU-241224/1521

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K" The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110 At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe0891080f8cab7890. **CVE ID : CVE-2024-53127**	0bff71745bc3583bd5ca59be91e0ee1d27f1944, https://git.kernel.org/stable/c/1635e407a4a64d08a8517ac59ca14ad4fc785e75, https://git.kernel.org/stable/c/56de724c58c07a7ca3aac027cfd2ccb184ed9e4e	
Affected Version(s): From (including) 6.1.116 Up to (excluding) 6.1.119					
Concurrent Execution using Shared Resource with Improper	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35	O-LIN-LINU-241224/1522

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	d88a3a294443e32d52, https://git.kernel.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	
Affected Version(s): From (including) 6.1.60 Up to (excluding) 6.1.119					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted	https://git.kernel.org/stable/c/581302298524e9d77c4c44ff5156a6cd112227ae, https://git.kernel.org/stable/c/955388e1d5d222c4101c596b536d41b91a8	O-LIN-LINU-241224/1523

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:__tcp_select_window+0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80 R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000)	b212e, https://git.kernel.org/stable/c/a66805c9b22caf4e42af7a616f6c6b83c90d1010	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289 inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline] __se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_syscall_x64 arch/x86/entry/common.c: 52 [inline] do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559 RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and provided a nice reproducer. The root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss. Catch the error and return without performing any additional operations on the current socket. **CVE ID : CVE-2024-53123**		
Affected Version(s): From (including) 6.10 Up to (excluding) 6.11.10					
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix handling of partial GPU mapping of BOs This commit fixes the bug in the handling of partial mapping of the buffer objects to the GPU, which caused kernel warnings. Panthor didn't correctly handle the case where the partial mapping	https://git.kernel.org/stable/c/3387e043918e154ca08d83954966a8b087fe2835, https://git.kernel.org/stable/c/d3e61af64b770e0038470c81f42bd1d0598f6bcc	O-LIN-LINU-241224/1524

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spanned multiple scatterlists and the mapping offset didn't point to the 1st page of starting scatterlist. The offset variable was not cleared after reaching the starting scatterlist. Following warning messages were seen. WARNING: CPU: 1 PID: 650 at drivers/iommu/io-pgtable-arm.c:659 __arm_lpae_unmap+0x254/0x5a0 <snip> pc : __arm_lpae_unmap+0x254/0x5a0 lr : __arm_lpae_unmap+0x2cc/0x5a0 <snip> Call trace: __arm_lpae_unmap+0x254/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arm_lpae_unmap_pages+0x80/0xa0 panthor_vm_unmap_pages+0xac/0x1c8 [panthor] panthor_gpuva_sm_step_unmap+0x4c/0xc8 [panthor] op_unmap_cb.isra.23.constprop.30+0x54/0x80 __drm_gpuvm_sm_unmap+0x184/0x1c8 drm_gpuvm_sm_unmap+0x40/0x60 panthor_vm_exec_op+0xa8/0x120 [panthor] panthor_vm_bind_exec_sync_op+0xc4/0xe8 [panthor] panthor_ioctl_vm_bind+0x10c/0x170 [panthor] drm_ioctl_kernel+0xbc/0x138 drm_ioctl+0x210/0x4b0 __arm64_sys_ioctl+0xb0/0xf8 invoke_syscall+0x4c/0x110 el0_svc_common.constprop.1+0x98/0xf8 do_el0_svc+0x24/0x38		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			el0_svc+0x34/0xc8 el0t_64_sync_handler+0xa0/0xc8 el0t_64_sync+0x174/0x178 <snip> panthor : [drm] drm_WARN_ON(unmapped_sz != pgsize * pgcount) WARNING: CPU: 1 PID: 650 at drivers/gpu/drm/panthor/panthor_mmu.c:922 panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip> pc : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] lr : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip> panthor : [drm] *ERROR* failed to unmap range ffffa388f000-ffffa3890000 (requested range ffffa388c000-ffffa3890000) **CVE ID : CVE-2024-53116**		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ARM: fix cacheflush with PAN	https://git.kernel.org/stable/c/ca29cfcc4a21083d671522ad384532e28a43f033, https://	O-LIN-LINU-241224/1525

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It seems that the cacheflush syscall got broken when PAN for LPAE was implemented. User access was not enabled around the cache maintenance instructions, causing them to fault. **CVE ID : CVE-2024-53137**	git.kernel.org/stable/c/e6960a2ed49c9a25357817535f7cc50594a58604	
Affected Version(s): From (including) 6.10.4 Up to (excluding) 6.11					
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: avoid null_ptr_deref in vmw_framebuffer_surface_create_handle The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_create_handle. **CVE ID : CVE-2024-53115**	https://git.kernel.org/stable/c/36f64da080555175b58d85f99f5f90435e274e56, https://git.kernel.org/stable/c/93d1f41a82de382845af460bf03bcb17dcbf08c5	O-LIN-LINU-241224/1526
Affected Version(s): From (including) 6.11 Up to (excluding) 6.11.10					
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: avoid null_ptr_deref in	https://git.kernel.org/stable/c/36f64da080555175b58d85f99f5f	O-LIN-LINU-241224/1527

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vmw_framebuffer_surface_create_handle The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_create_handle. **CVE ID : CVE-2024-53115**	90435e274e56, https://git.kernel.org/stable/c/93d1f41a82de382845af460bf03bcb17dcbf08c5	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K" The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110	https://git.kernel.org/stable/c/00bff71745bc3583bd5ca59be91e0ee1d27f1944, https://git.kernel.org/stable/c/1635e407a4a64d08a8517ac59ca14ad4fc785e75, https://git.kernel.org/stable/c/56de724c58c07a7ca3aac027cfd2c	O-LIN-LINU-241224/1528

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe0891080f8cab7890. **CVE ID : CVE-2024-53127**	cb184ed9e4e	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix "Missing outer runtime PM protection" warning Fix the following drm_WARN: [953.586396] xe 0000:00:02.0: [drm] Missing outer runtime PM protection ... <4> [953.587090] ? xe_pm_runtime_get_noresume+0x8d/0xa0 [xe] <4> [953.587208] guc_exec_queue_add_msg+0x28/0x130 [xe] <4> [953.587319] guc_exec_queue_fini+0x3a/0x40 [xe] <4> [953.587425] xe_exec_queue_destroy+0xb3/0xf0 [xe]	https://git.kernel.org/stable/c/c0403e4ceecaefbeaf78263dffcd3e3f06a19f6b, https://git.kernel.org/stable/c/ed7cd3510d8da6e3578d9125a9ea4440f8adeeaa	O-LIN-LINU-241224/1529

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<4> [953.587515] xe_oa_release+0x9c/0xc0 [xe] (cherry picked from commit b107c63d2953907908fd0cafb0e543b3c3167b75) **CVE ID : CVE-2024-53132**		
Affected Version(s): From (including) 6.11.0 Up to (excluding) 6.11.10					
N/A	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is placed on the stack. Neither pcim_iomap_regions() nor the functions it calls copy that string. Should the string later ever be used, this, consequently, causes undefined behavior since the stack frame will by then have disappeared. Fix the bug by allocating the strings on the heap through devm_kasprintf(). **CVE ID : CVE-2024-53126**	https://git.kernel.org/stable/c/0b364cf53b20204e92bac7c6ebd1ee7d3ec62931, https://git.kernel.org/stable/c/5bb287da2d2d5bb8f7376e223b02edb16998982e, https://git.kernel.org/stable/c/d372dd09cfbf1324f54cbffd81fcaf6cdf3e608e	O-LIN-LINU-241224/1530

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip/rockchip_drm_vop.c:1096 vop_plane_atomic_async_check() warn: variable dereferenced before check 'state' (see line 1077) **CVE ID : CVE-2024-53129**	https://git.kernel.org/stable/c/1e53059729691ca4d905118258b9fbd17d854174, https://git.kernel.org/stable/c/656dbd1c21c2c088c70059cdd43ec83e7d54ec4d, https://git.kernel.org/stable/c/ab1c793f457f740ab7108cc0b1340a402dbf484d	O-LIN-LINU-241224/1531
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer" tracepoint, mark_buffer_dirty()	https://git.kernel.org/stable/c/2026559a6c4ce34db117d2db8f710fe2a9420d5a, https://git.kernel.org/stable/c/7a	O-LIN-LINU-241224/1532

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b-tree node blocks, does not set the block device, but instead does so only if the buffer is not in the "uptodate" state for each of its caller block reading functions. However, if the uptodate flag is set on a folio/page, and the buffer heads are detached from it by try_to_free_buffers(), and new buffer heads are then attached by create_empty_buffers(), the uptodate flag may	f3309c7a2ef26831a67125b11c34a7e01c1b2a, https://git.kernel.org/stable/c/86b19031dbc79abc378dfae357f6ea33ebeb0c95	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be restored to each buffer without the block device being set to bh->b_bdev, and mark_buffer_dirty() may be called later in that state, resulting in the bug mentioned above. Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag. **CVE ID : CVE-2024-53130**		
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint Patch series "nilfs2: fix null-ptr-deref bugs on block tracepoints". This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints. This patch (of 2):	https://git.kernel.org/stable/c/085556bf8c70e2629e02e79268dac3016a08b8bf, https://git.kernel.org/stable/c/3b2a4fd9bbee77afdd3ed5a05a0c02b6cde8d3b9, https://git.kernel.org/stable/c/5	O-LIN-LINU-241224/1533

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			It has been reported that when using "block:block_touch_buffer" tracepoint, touch_buffer() called from __nilfs_get_folio_block() causes a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because since the tracepoint was added in touch_buffer(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, the block_device structure is set after the function returns to the caller. Here, touch_buffer() is used to mark the folio/page that owns the buffer head as accessed, but the common search helper for folio/page used by the caller function was optimized to mark the folio/page as accessed when it	9b49ca67cca7b007a5afd3de0283c8008157665	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			was reimplemented a long time ago, eliminating the need to call touch_buffer() here in the first place. So this solves the issue by eliminating the touch_buffer() call itself. **CVE ID : CVE-2024-53131**		
Affected Version(s): From (including) 6.11.7 Up to (excluding) 6.11.10					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kernel.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	O-LIN-LINU-241224/1534

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 6.12 Up to (excluding) 6.12.2					
N/A	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE ID : CVE-2024-53141**	https://git.kernel.org/stable/c/15794835378ed56fb9bacc6a5dd3b9f33520604e, https://git.kernel.org/stable/c/35f56c554eb1b56b77b3cf197a6b00922d49033d, https://git.kernel.org/stable/c/3c20b5948f119ae61ee35ad8584d666020c91581	O-LIN-LINU-241224/1535
Out-of-bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in	https://git.kernel.org/stable/c/1a423bbbeaf9e3e20c4686501efd9b661fe834db, https://git.kerne	O-LIN-LINU-241224/1536

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Documentation/driver-api/early-userspace/buffer-format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data ... 55 ============= ================== ===================== ==== 56 Field name Field size Meaning 57 ============= ================== ===================== ==== ... 70 c_namesize 8 bytes Length of filename, including final \0 When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero-terminated path at @collected, passing it directly to filp_open() / init_mkdir() / init_mknod(). If a specially crafted cpio entry carries a non-zero-terminated filename and is followed by uninitialized memory, then a file may be created with	l.org/stable/c/49d01e736c3045319e030d1e75fb983011abaca7, https://git.kernel.org/stable/c/bb7ac96670ab1d8d681015f9d66e45dad579af4d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			trailing characters that represent the uninitialized memory. The ability to create an initramfs entry would imply already having full control of the system, so the buffer overrun shouldn't be considered a security vulnerability.
			
			Append the output of the following bash script to an existing initramfs and observe any created /initramfs_test_fname_overrunAA* path. E.g.
			./reproducer.sh | gzip >> /myinitramfs
			
			It's easiest to observe non-zero uninitialized memory when the output is gzipped, as it'll overflow the heap allocated @out_buf in __gunzip(), rather than the initrd_start+initrd_size block.
			
			---- reproducer.sh ----
			nilchar="A" # change to "\0" to properly zero terminate / pad
			magic="070701"
			ino=1
			mode=$((0100777))
			uid=0		

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			gid=0 nlink=1 mtime=1 filesize=0 devmajor=0 devminor=1 rdevmajor=0 rdevminor=0 csum=0 fname="initramfs_test_fname_overrun" namelen=$((${#fname} + 1)) # plus one to account for terminator printf "%s%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%s" \ $magic $ino $mode $uid $gid $nlink $mtime $filesize \ $devmajor $devminor $rdevmajor $rdevminor $namelen $csum $fname termpadlen=$((1 + ((4 - ((110 + $namelen) & 3)) % 4))) printf "%.s${nilchar}" $(seq 1 $termpadlen) ---- reproducer.sh ----		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Symlink filename fields handled in do_symlink() won't overrun past the data segment, due to the explicit zero-termination of the symlink target. Fix filename buffer overrun by aborting the initramfs FSM if any cpio entry doesn't carry a zero-terminator at the expected (name_len - 1) offset. **CVE ID : CVE-2024-53142**		
Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.63					
Use After Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST=y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] =============================	https://git.kernel.org/stable/c/05656a66592759242c74063616291b7274d11b2f, https://git.kernel.org/stable/c/ad975697211f4f2c4ce61c3ba524fd14d88ceab8, https://git.kernel.org/stable/c/eb	O-LIN-LINU-241224/1537

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W ----------------------------- net/core/dev.c:876 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by sctp_hello/31495: #0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}-{0:0}, at: sctp_bind (./arch/x86/include/asm/jump_label.h:27 net/sctp/socket.c:315) sctp stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5-virtme #1216 Tainted: [W]=WARN Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123)	72e7fcc 83987d 5d5595 b43222f 23b295 d5de7f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lockdep_rcu_suspicious (kernel/locking/lockdep.c:6822) dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7)) sctp_v6_available (net/sctp/ipv6.c:701) sctp sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp sctp_bind (net/sctp/socket.c:320) sctp inet6_bind_sk (net/ipv6/af_inet6.c:465) ? security_socket_bind (security/security.c:4581 (discriminator 1)) __sys_bind (net/socket.c:1848 net/socket.c:1869) ? do_user_addr_fault (./include/linux/rcupdate.h:347 ./include/linux/rcupdate.h:880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) ? do_user_addr_fault (./arch/x86/include/asm/preempt.h:84 (discriminator 13) ./include/linux/rcupdate.h:98 (discriminator 13) ./include/linux/rcupdate.h:882 (discriminator 13) ./include/linux/mm.h:729 (discriminator 13) arch/x86/mm/fault.c:1340 (discriminator 13))		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1) arch/x86/entry/common.c:83 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48 All code ======== 0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00 mov 0xc8c39(%rip),%rdx # 0xc8c43 a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f: b8 ff ff ff ff mov $0xffffffff,%eax 14: eb bd jmp 0xffffffffffffffd3 16: 66 2e 0f 1f 84 00 00 cs nopw 0x0(%rax,%rax,1) 1d: 00 00 00 20: 0f 1f 00 nopl (%rax) 23: b8 31 00 00 00 mov $0x31,%eax 28: 0f 05 syscall 2a:* 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax <-- trapping instruction 30: 73 01 jae 0x33 32: c3 ret 33: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c43 3a: f7 d8 neg %eax 3c: 64 89 01 mov %eax,%fs:(%rcx) 3f: 48 rex.W Code starting with the faulting instruction ===		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0: 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax 6: 73 01 jae 0x9 8: c3 ret 9: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c19 10: f7 d8 neg %eax 12: 64 89 01 mov %eax,%fs:(%rcx) 15: 48 rex.W RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 0000000000000031 RAX: ffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7 RDX: 000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 0000000000000005 RBP: 0000000000000005 R08: 1999999999999999 R09: 0000000000000000 R10: 00007f59b9253298 R11: 000000000000 ---truncated--- **CVE ID : CVE-2024-53139**		
N/A	04-Dec-2024	6.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/aa0d42cac	O-LIN-LINU-241224/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the implementation, some of which are fatal to the guest, and others which put the stability and health of the host at risk. For guest fatalities, the most glaring issue is that KVM fails to ensure tracing is disabled, and *stays* disabled prior to VM-Enter, which is necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing is enabled (enforced via a VMX consistency check). Per the SDM: If the logical processor is operating with Intel PT enabled (if IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load	f093a6fcca872edc954f6f812926a17, https://git.kernel.org/stable/c/b91bb0ce5cd7005b376eac690ec664c1b56372ec, https://git.kernel.org/stable/c/d28b059ee4779b5102c5da6e929762520510e406	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IA32_RTIT_CTL" VM-entry control must be 0. On the host side, KVM doesn't validate the guest CPUID configuration provided by userspace, and even worse, uses the guest configuration to decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring guest CPUID to enumerate more address ranges than are supported in hardware will result in KVM trying to passthrough, save, and load non-existent MSRs, which generates a variety of WARNs, ToPA ERRORs in the host, a potential deadlock, etc. **CVE ID : CVE-2024-53135**		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. **CVE ID : CVE-2024-53110**	https://git.kernel.org/stable/c/0a886489d274596ad1a80789d3a773503210a615, https://git.kernel.org/stable/c/4e39ecadf1d2a08187139619f1f31	O-LIN-LINU-241224/1539

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4b64ba7d947, https://git.kernel.org/stable/c/870d68fe17b5d9032049dcad98b5781a344a8657	
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? do_error_trap+0x1dc/0x2c0	https://git.kernel.org/stable/c/620d22598110b0d0cb97a3fcca65fc473ea86e73, https://git.kernel.org/stable/c/737f34137844d6572ab7d473c998c7f977ff30eb, https://git.kernel.org/stable/c/843dfc804af4b338ead42331dd58081b428ecdf8	O-LIN-LINU-241224/1540

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10 ? handle_invalid_op+0x34/0x40 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160 ? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10 ? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160 ? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0 ? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780 ? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... </TASK> When 'ioctl(OCFS2_IOC_GROUP_ADD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'. **CVE ID : CVE-2024-53112**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof	https://git.kernel.org/stable/c/31502374627ba9ec3e710dbd0bb00457cc6d2c19, https://	O-LIN-LINU-241224/1541

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets. When cpuset is enabled, in prepare_alloc_pages(), ac->nodemask may be &current->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac->nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node, when traversing Node1 in ac->zonelist, the nodemask is 2, and when traversing Node2 in ac->zonelist, the nodemask is 1. As a result, the ac->preferred_zoneref points to NULL zone. In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nodemask() finds a allowable zone and calls zonelist_node_idx(ac.preferred_zoneref), leading to NULL pointer dereference.	git.kernel.org/stable/c/6addb2d9501ec866d7b3a3b4e665307c437e9be2, https://git.kernel.org/stable/c/8ce41b0f9d77cca074df25afd39b86e2ee3aa68e	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__alloc_pages_noprof() fixes this issue by checking NULL pointer in commit ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath"). To fix it, check NULL pointer for preferred_zoneref->zone. **CVE ID : CVE-2024-53113**		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Fix accept_queue memory leak As the final stages of socket destruction may be delayed, it is possible that virtio_transport_recv_listen() will be called after the accept_queue has been flushed, but before the SOCK_DONE flag has been set. As a result, sockets enqueued after the flush would remain unremoved, leading to a memory leak.	https://git.kernel.org/stable/c/2415345042245de7601dcc6eafdbe3a3dcc9e379, https://git.kernel.org/stable/c/897617a413e0bf1c6380e3b34b2f28f450508549, https://git.kernel.org/stable/c/946c7600fa2207c	O-LIN-LINU-241224/1542

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	vsock_release __vsock_release lock virtio_transport_release virtio_transport_close schedule_delayed_work(close_work) sk_shutdown = SHUTDOWN_MASK (!) flush accept_queue release virtio_transport_recv_pkt vsock_find_bound_socket lock if flag(SOCK_DONE) return virtio_transport_recv_listen child = vsock_create_connected (!) vsock_enqueue_accept(child) release close_work lock virtio_transport_do_close set_flag(SOCK_DONE) virtio_transport_remove_sock vsock_remove_sock	c8d3fbc86a518ec56f98a5813	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_remove_bound release Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction. unreferenced object 0xffff888109e3f800 (size 2040): comm "kworker/5:2", pid 371, jiffies 4294940105 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 (..@............ backtrace (crc 9e5f4e84): [<ffffffff81418ff1>] kmem_cache_alloc_noprof+0x2c1/0x360 [<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120 [<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0 [<ffffffff81fe049a>] __vsock_create.constprop.0+0x2a/0x310 [<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0x4dc/0x9a0 [<ffffffff81fe745d>] vsock_loopback_work+0xfd/0x140		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff810fc6ac>] process_one_work+0x20c/0x570 [<ffffffff810fce3f>] worker_thread+0x1bf/0x3a0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<ffffffff81044fdd>] ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0x30 **CVE ID : CVE-2024-53119**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr-deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule(), in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000110 RIP: 0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core]	https://git.kernel.org/stable/c/06dc488a593020bd2f006798557d2a32104d8359, https://git.kernel.org/stable/c/0c7c70ff8b696cfedba350411dca736361ef9a0f, https://git.kernel.org/stable/c/6030f8bd7902e9e276a0edc09bf11	O-LIN-LINU-241224/1543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	... Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0x30 ? mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] ? mlx5_tc_ct_entry_add_rule+0x1d5/0x2f0 [mlx5_core] mlx5_tc_ct_block_flow_offload+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] flow_offload_work_handler+0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x15b/0x2b0 process_one_work+0x16c/0x320	979e4e2bc2e	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker_thread+0x28c/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xb8/0xf0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> **CVE ID : CVE-2024-53120**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray.	https://git.kernel.org/stable/c/094d1a2121cee1e85ab07d74388f94809dcfb5b9, https://git.kernel.org/stable/c/933ef0d17f012b653e9e6006e3f50c8d0238b5ed, https://git.kernel.org/stable/c/9c	O-LIN-LINU-241224/1544

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely, causing a panic during subsequent rule deletions. To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to an FTE that is in the process of deletion. [438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func [438.968205] ------------[cut here]------------ [438.968654] refcount_t: decrement hit 0; leaking memory. [438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xfb/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch	a314419930f9135727e39d77e66262d5f7bef6	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower] [438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [438.974874] RIP: 0010:refcount_warn_saturate+0xfb/0x110 [438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90 [438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286 [438.977446] RAX: 0000000000000000 RBX:		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff888119d56de0 RCX: 0000000000000000 [438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0 [438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0 [438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0 [438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0 [438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:0000000000000000 [438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 0000000000372eb0 [438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [438.985842] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [438.986507] Call Trace: [438.986799] <TASK>		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.987070] ? __warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xfb/0x110 [438.987877] ? report_bug+0x17d/0x190 [438.988261] ? prb_read_valid+0x17/0x20 [438.988659] ? handle_bug+0x53/0x90 [438.989054] ? exc_invalid_op+0x14/0x70 [438.989458] ? asm_exc_invalid_op+0x16/0x20 [438.989883] ? refcount_warn_saturate+0xfb/0x110 [438.990348] mlx5_del_flow_rules+0x2f7/0x340 [mlx5_core] [438.990932] __mlx5_eswitch_del_rule+0x49/0x170 [mlx5_core] [438.991519] ? mlx5_lag_is_sriov+0x3c/0x50 [mlx5_core] [438.992054] ? xas_load+0x9/0xb0 [438.992407] mlx5e_tc_rule_unoffload+0x45/0xe0 [mlx5_core] [438.993037] mlx5e_tc_del_fdb_flow+0x2a6/0x2e0 [mlx5_core] [438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261/0x390 [mlx5_core] [438.994728] tc_setup_cb_destroy+0xb9/0x190 [438.995150] fl_hw_destroy_filter+0x94/0xc0 [cls_flower] [438.995650] fl_change+0x11a4/0x13c0 [cls_flower] [438.996105] tc_new_tfilter+0x347/0xbc0 [438.996503] ? __ ---truncated--- **CVE ID : CVE-2024-53121**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: cope racing subflow creation in mptcp_rcv_space_adjust Additional active subflows - i.e. created by the in kernel path manager - are included into the subflow list before starting the 3whs. A racing recvmsg() spooling data received on an already established subflow would unconditionally call	https://git.kernel.org/stable/c/24995851d58c4a205ad0ffa7b2f21e479a9c8527, https://git.kernel.org/stable/c/aad6412c63baa39dd813e81f16a14d976b3de2e8, https://git.kernel.org/stable/c/ce	O-LIN-LINU-241224/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). **CVE ID : CVE-2024-53122**	7356ae35943cc6494cc692e62d51a734062b7d	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resync_dump_comp()), only put_page() is used. This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc()	https://git.kernel.org/stable/c/2723e8b2cbd486cb96e5a61b22473f7fd62e18df, https://git.kernel.org/stable/c/69fbd07f17b0fdaf8970bc705f5bf115c297839d, https://git.kernel.org/stable/c/93a14620b97c911489a5b008782f3	O-LIN-LINU-241224/1546

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			references are stored directly in the given page. On release the folio page will be dereferenced too many times. This was found while doing kTLS testing with sendfile() + ZC when the served file was read from NFS on a kernel with NFS large folios support (commit 49b29a573da8 ("nfs: add support for large folios")). **CVE ID : CVE-2024-53138**	d9b0c4aeff4	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup	https://git.kernel.org/stable/c/114a61d8d94ae3a43b82446cf737fd757021b834, https://git.kernel.org/stable/c/176c41b3ca9281a9736b67c6121b03dbf0c8c08f, https://git.kernel.org/stable/c/1904fb9ebf91144	O-LIN-LINU-241224/1547

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket. This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone	1f90a68e96b22aa73e4410505	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			else holds the socket they may release it in BH and we're back to square one. The whole dance, however, appears to be unnecessary. Only the user can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own. **CVE ID : CVE-2024-53140**		
Affected Version(s): From (including) 6.5.9 Up to (excluding) 6.6					
Concurrent Execution using Shared Resource	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/5813022	O-LIN-LINU-241224/1548

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:__tcp_select_window+0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b	98524e9d77c4c44ff5156a6cd112227ae, https://git.kernel.org/stable/c/955388e1d5d222c4101c596b536d41b91a8b212e, https://git.kernel.org/stable/c/a66805c9b22caf4e42af7a616f6c6b83c90d1010	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80 R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline] __se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef and provided a nice reproducer. The root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss. Catch the error and return without performing any additional operations on the current socket. **CVE ID : CVE-2024-53123**		
Affected Version(s): From (including) 6.6 Up to (excluding) 6.6.63					
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/247d720b2c5d22	O-LIN-LINU-241224/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nommu: pass NULL argument to vma_iter_prealloc() When deleting a vma entry from a maple tree, it has to pass NULL to vma_iter_prealloc() in order to calculate internal state of the tree, but it passed a wrong argument. As a result, nommu kernels crashed upon accessing a vma iterator, such as acct_collect() reading the size of vma entries after do_munmap(). This commit fixes this issue by passing a right argument to the preallocation call. **CVE ID : CVE-2024-53109**	f7281437fd6054a138256986ba, https://git.kernel.org/stable/c/8bbf0ab631cdf1dade6745f137cff98751e6ced7, https://git.kernel.org/stable/c/aceaf33b7666b72dfb86e0aa977be81e3bcbc727	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI	https://git.kernel.org/stable/c/581302298524e9d77c4c44ff5156a6cd112227ae, https://git.kernel.org/stable/c/955388e1d5d222c4101c59	O-LIN-LINU-241224/1550

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟨	CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:__tcp_select_window+0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80	6b536d41b91a8b212e, https://git.kernel.org/stable/c/a66805c9b22caf4e42af7a616f6c6b83c90d1010	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289 inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline]		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559 RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef and provided a nice reproducer. The root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss. Catch the error and return without performing any additional operations on the current socket. **CVE ID : CVE-2024-53123**		
Affected Version(s): From (including) 6.6.0 Up to (excluding) 6.6.63					
N/A	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is placed on the stack. Neither	https://git.kernel.org/stable/c/0b364cf53b20204e92bac7c6ebd1ee7d3ec62931, https://git.kernel.org/stable/c/5bb287da2d2d5b	O-LIN-LINU-241224/1551

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pcim_iomap_regions() nor the functions it calls copy that string. Should the string later ever be used, this, consequently, causes undefined behavior since the stack frame will by then have disappeared. Fix the bug by allocating the strings on the heap through devm_kasprintf(). **CVE ID : CVE-2024-53126**	b8f7376e223b02edb16998982e, https://git.kernel.org/stable/c/d372dd09cfbf1324f54cbffd81fcaf6cdf3e608e	
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip/rockchip_drm_vop.c:1096 vop_plane_atomic_async_check() warn: variable dereferenced before check 'state' (see line 1077) **CVE ID : CVE-2024-53129**	https://git.kernel.org/stable/c/1e53059729691ca4d905118258b9fbd17d854174, https://git.kernel.org/stable/c/656dbd1c21c2c088c70059cdd43ec83e7d54ec4d, https://git.kernel.org/stable/c/ab1c793f457f740a	O-LIN-LINU-241224/1552

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b7108cc0b1340a402dbf484d	
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer" tracepoint, mark_buffer_dirty() may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b-tree node blocks,	https://git.kernel.org/stable/c/2026559a6c4ce34db117d2db8f710fe2a9420d5a, https://git.kernel.org/stable/c/7af3309c7a2ef26831a67125b11c34a7e01c1b2a, https://git.kernel.org/stable/c/86b19031dbc79abc378dfae357f6ea33ebeb0c95	O-LIN-LINU-241224/1553

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not set the block device, but instead does so only if the buffer is not in the "uptodate" state for each of its caller block reading functions. However, if the uptodate flag is set on a folio/page, and the buffer heads are detached from it by try_to_free_buffers(), and new buffer heads are then attached by create_empty_buffers(), the uptodate flag may be restored to each buffer without the block device being set to bh->b_bdev, and mark_buffer_dirty() may be called later in that state, resulting in the bug mentioned above. Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag. **CVE ID : CVE-2024-53130**		
NULL Pointer Dereference	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/085556bf8c70e2629e02e7	O-LIN-LINU-241224/1554

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint Patch series "nilfs2: fix null-ptr-deref bugs on block tracepoints". This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints. This patch (of 2): It has been reported that when using "block:block_touch_buffer" tracepoint, touch_buffer() called from __nilfs_get_folio_block() causes a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because since the tracepoint was added in touch_buffer(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the	9268dac3016a08b8bf, https://git.kernel.org/stable/c/3b2a4fd9bbee77afdd3ed5a05a0c02b6cde8d3b9, https://git.kernel.org/stable/c/59b49ca67cca7b007a5afd3de0283c8008157665	

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 head has a pointer to a block_device structure. In the current implementation, the block_device structure is set after the function returns to the caller. Here, touch_buffer() is used to mark the folio/page that owns the buffer head as accessed, but the common search helper for folio/page used by the caller function was optimized to mark the folio/page as accessed when it was reimplemented a long time ago, eliminating the need to call touch_buffer() here in the first place. So this solves the issue by eliminating the touch_buffer() call itself. **CVE ID : CVE-2024-53131**		
Affected Version(s): From (including) 6.6.51 Up to (excluding) 6.6.63					
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K"	https://git.kernel.org/stable/c/00bff71745bc3583bd5ca59be91e0ee1d27f1944, https://	O-LIN-LINU-241224/1555

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110 At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe0891080f8cab7890. **CVE ID : CVE-2024-53127**	git.kernel.org/stable/c/1635e407a4a64d08a8517ac59ca14ad4fc785e75, https://git.kernel.org/stable/c/56de724c58c07a7ca3aac027cfd2ccb184ed9e4e	
Affected Version(s): From (including) 6.6.60 Up to (excluding) 6.6.63					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-Dec-2024	4.7	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()"	https://git.kernel.org/stable/c/36b537e8f302f670c7cf35d88a3a294443e32d52, https://git.kerne	O-LIN-LINU-241224/1556

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem". **CVE ID : CVE-2024-53136**	l.org/stable/c/5874c1150e77296565ad6e495ef41fbf87570d14, https://git.kernel.org/stable/c/64e67e8694252c1bf01b802ee911be3fee62c36b	
Affected Version(s): From (including) 6.7 Up to (excluding) 6.11.10					
Use After Free	04-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST=y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] ============================	https://git.kernel.org/stable/c/05656a66592759242c74063616291b7274d11b2f, https://git.kernel.org/stable/c/ad975697211f4f2c4ce61c3ba524fd14d88ceab8, https://git.kernel.org/stable/c/eb	O-LIN-LINU-241224/1557

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W ----------------------------- net/core/dev.c:876 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by sctp_hello/31495: #0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}-{0:0}, at: sctp_bind (./arch/x86/include/asm/jump_label.h:27 net/sctp/socket.c:315) sctp stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5-virtme #1216 Tainted: [W]=WARN Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123)	72e7fcc83987d5d5595b43222f23b295d5de7f	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lockdep_rcu_suspicious (kernel/locking/lockdep.c:6822) dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7)) sctp_v6_available (net/sctp/ipv6.c:701) sctp sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp sctp_bind (net/sctp/socket.c:320) sctp inet6_bind_sk (net/ipv6/af_inet6.c:465) ? security_socket_bind (security/security.c:4581 (discriminator 1)) __sys_bind (net/socket.c:1848 net/socket.c:1869) ? do_user_addr_fault (./include/linux/rcupdate.h:347 ./include/linux/rcupdate.h:880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) ? do_user_addr_fault (./arch/x86/include/asm/preempt.h:84 (discriminator 13) ./include/linux/rcupdate.h:98 (discriminator 13) ./include/linux/rcupdate.h:882 (discriminator 13) ./include/linux/mm.h:729 (discriminator 13) arch/x86/mm/fault.c:1340 (discriminator 13))		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			__x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1) arch/x86/entry/common.c:83 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48 All code ======== 0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00 mov 0xc8c39(%rip),%rdx # 0xc8c43 a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx)		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			f: b8 ff ff ff ff mov $0xffffffff,%eax 14: eb bd jmp 0xffffffffffffffd3 16: 66 2e 0f 1f 84 00 00 cs nopw 0x0(%rax,%rax,1) 1d: 00 00 00 20: 0f 1f 00 nopl (%rax) 23: b8 31 00 00 00 mov $0x31,%eax 28: 0f 05 syscall 2a:* 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax <-- trapping instruction 30: 73 01 jae 0x33 32: c3 ret 33: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c43 3a: f7 d8 neg %eax 3c: 64 89 01 mov %eax,%fs:(%rcx) 3f: 48 rex.W Code starting with the faulting instruction ===		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			0: 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax 6: 73 01 jae 0x9 8: c3 ret 9: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c19 10: f7 d8 neg %eax 12: 64 89 01 mov %eax,%fs:(%rcx) 15: 48 rex.W RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 0000000000000031 RAX: ffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7 RDX: 000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 0000000000000005 RBP: 0000000000000005 R08: 1999999999999999 R09: 0000000000000000 R10: 00007f59b9253298 R11: 000000000000 ---truncated--- **CVE ID : CVE-2024-53139**		
Out-of-bounds Read	02-Dec-2024	7.1	In the Linux kernel, the following vulnerability has been resolved:	https://git.kernel.org/stable/c/0a326fbc8f	O-LIN-LINU-241224/1558

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			drm/amd/display: Adjust VSDB parser for replay feature At some point, the IEEE ID identification for the replay check in the AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN: [27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesync_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 ... [27.821207] Memory state around the buggy address: [27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc	72a320051f27328d4d4e7abdfe68d7, https://git.kernel.org/stable/c/16dd2825c23530f2259fc671960a3a65d2af69bd, https://git.kernel.org/stable/c/8db867061f4c76505ad62422b65d666b45289217	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821268] == This is caused because the ID extraction happens outside of the range of the edid lenght. This commit addresses this issue by considering the amd_vsdb_block size. (cherry picked from commit b7e381b1ccd5e778e3d9c44c669ad38439a861d8) **CVE ID : CVE-2024-53108**		
N/A	04-Dec-2024	6.5	In the Linux kernel, the following vulnerability has been resolved: KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support	https://git.kernel.org/stable/c/aa0d42cacf093a6fcca872edc954f6f812926a17, https://git.kernel.org/stable/c/b	O-LIN-LINU-241224/1559

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the implementation, some of which are fatal to the guest, and others which put the stability and health of the host at risk. For guest fatalities, the most glaring issue is that KVM fails to ensure tracing is disabled, and *stays* disabled prior to VM-Enter, which is necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing is enabled (enforced via a VMX consistency check). Per the SDM: If the logical processor is operating with Intel PT enabled (if IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load IA32_RTIT_CTL" VM-entry control must be 0. On the host side, KVM doesn't validate the guest CPUID configuration provided by userspace, and even worse, uses the guest configuration to	91bb0ce5cd7005b376eac690ec664c1b56372ec, https://git.kernel.org/stable/c/d28b059ee4779b5102c5da6e929762520510e406	

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring guest CPUID to enumerate more address ranges than are supported in hardware will result in KVM trying to passthrough, save, and load non-existent MSRs, which generates a variety of WARNs, ToPA ERRORs in the host, a potential deadlock, etc. **CVE ID : CVE-2024-53135**		
Integer Overflow or Wraparound	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: prevent integer overflow in pagemap_scan_get_args() The "arg->vec_len" variable is a u64 that comes from the user at the start of the function. The "arg->vec_len * sizeof(struct page_region))" multiplication can lead to integer wrapping. Use size_mul() to avoid that. Also the size_add/mul() functions work on unsigned long so for 32bit	https://git.kernel.org/stable/c/669b0cb81e4e4e78cff77a5b367c7f70c0c6c05e, https://git.kernel.org/stable/c/adee03f8903c58a6a559f21388a430211fac8ce9	O-LIN-LINU-241224/1560

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems we need to ensure that "arg->vec_len" fits in an unsigned long. **CVE ID : CVE-2024-53107**		
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: nommu: pass NULL argument to vma_iter_prealloc() When deleting a vma entry from a maple tree, it has to pass NULL to vma_iter_prealloc() in order to calculate internal state of the tree, but it passed a wrong argument. As a result, nommu kernels crashed upon accessing a vma iterator, such as acct_collect() reading the size of vma entries after do_munmap(). This commit fixes this issue by passing a right argument to the preallocation call. **CVE ID : CVE-2024-53109**	https://git.kernel.org/stable/c/247d720b2c5d22f7281437fd6054a138256986ba, https://git.kernel.org/stable/c/8bbf0ab631cdf1dade6745f137cff98751e6ced7, https://git.kernel.org/stable/c/aceaf33b7666b72dfb86e0aa977be81e3bcbc727	O-LIN-LINU-241224/1561
N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vp_vdpa: fix id_table array not null terminated error	https://git.kernel.org/stable/c/0a886489d274596ad1a80789d3a7	O-LIN-LINU-241224/1562

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory. **CVE ID : CVE-2024-53110**	73503210a615, https://git.kernel.org/stable/c/4e39ecadf1d2a08187139619f1f314b64ba7d947, https://git.kernel.org/stable/c/870d68fe17b5d9032049dcad98b5781a344a8657	
Integer Overflow or Wraparound	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix address wraparound in move_page_tables() On 32-bit platforms, it is possible for the expression `len + old_addr < old_end` to be false-positive if `len + old_addr` wraps around. `old_addr` is the cursor in the old range up to which page table entries	https://git.kernel.org/stable/c/909543dc279a91122fb08e4653a72b82f0ad28f4, https://git.kernel.org/stable/c/a4a282daf1a190f03790bf163458ea3c8d28d217	O-LIN-LINU-241224/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been moved; so if the operation succeeded, `old_addr` is the *end* of the old region, and adding `len` to it can wrap. The overflow causes mremap() to mistakenly believe that PTEs have been copied; the consequence is that mremap() bails out, but doesn't move the PTEs back before the new VMA is unmapped, causing anonymous pages in the region to be lost. So basically if userspace tries to mremap() a private-anon region and hits this bug, mremap() will return an error and the private-anon region's contents appear to have been zeroed. The idea of this check is that `old_end - len` is the original start address, and writing the check that way also makes it easier to read; so fix the check by rearranging the comparison accordingly. (An alternate fix would be to refactor this function by introducing an "orig_old_start" variable or such.)		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

		🟨	Tested in a VM with a 32-bit X86 kernel; without the patch:
			```
			user@horn:~/big_mremap$ cat test.c
			#define _GNU_SOURCE
			#include <stdlib.h>
			#include <stdio.h>
			#include <err.h>
			#include <sys/mman.h>

			#define ADDR1 ((void*)0x60000000)
			#define ADDR2 ((void*)0x10000000)
			#define SIZE 0x50000000uL

			int main(void) {
			  unsigned char *p1 = mmap(ADDR1, SIZE, PROT_READ|PROT_WRITE,

			MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED_NOREPLACE, -1, 0);
			  if (p1 == MAP_FAILED)
			    err(1, "mmap 1");
			  unsigned char *p2 = mmap(ADDR2, SIZE, PROT_NONE,

			MAP_ANONYMOUS|MAP_PR
			```

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			IVATE|MAP_FIXED_NOREPLACE, -1, 0);
			 if (p2 == MAP_FAILED)
			   err(1, "mmap 2");
			 *p1 = 0x41;
			 printf("first char is 0x%02hhx\n", *p1);
			 unsigned char *p3 = mremap(p1, SIZE, SIZE,
			   MREMAP_MAYMOVE|MREMAP_FIXED, p2);
			 if (p3 == MAP_FAILED) {
			   printf("mremap() failed; first char is 0x%02hhx\n", *p1);
			 } else {
			   printf("mremap() succeeded; first char is 0x%02hhx\n", *p3);
			 }
			}
			user@horn:~/big_mremap$ gcc -static -o test test.c
			user@horn:~/big_mremap$ setarch -R ./test
			first char is 0x41
			mremap() failed; first char is 0x00
			```
			With the patch:
			```
			user@horn:~/big_mremap$ setarch -R ./test		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

			first char is 0x41
			mremap() succeeded; first char is 0x41
			```
			CVE ID : CVE-2024-53111
			```

N/A	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? do_error_trap+0x1dc/0x2c0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10	https://git.kernel.org/stable/c/620d22598110b0d0cb97a3fcca65fc473ea86e73, https://git.kernel.org/stable/c/737f34137844d6572ab7d473c998c7f977ff30eb, https://git.kernel.org/stable/c/843dfc804af4b338ead42331dd58081b428ecdf8	O-LIN-LINU-241224/1564

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_invalid_op+0x34/0x40 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160 ? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10 ? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0 ? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0 ? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780 ? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ...		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			</TASK> When 'ioctl(OCFS2_IOC_GROUP_ADD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'. **CVE ID : CVE-2024-53112**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets.	https://git.kernel.org/stable/c/31502374627ba9ec3e710dbd0bb00457cc6d2c19, https://git.kernel.org/stable/c/6addb2d9501ec866d7b3a3	O-LIN-LINU-241224/1565

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When cpuset is enabled, in prepare_alloc_pages(), ac->nodemask may be &current->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac->nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node, when traversing Node1 in ac->zonelist, the nodemask is 2, and when traversing Node2 in ac->zonelist, the nodemask is 1. As a result, the ac->preferred_zoneref points to NULL zone. In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nodemask() finds a allowable zone and calls zonelist_node_idx(ac.preferred_zoneref), leading to NULL pointer dereference. __alloc_pages_noprof() fixes this issue by checking NULL pointer in commit ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and	b4e665307c437e9be2, https://git.kernel.org/stable/c/8ce41b0f9d77cca074df25afd39b86e2ee3aa68e	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath"). To fix it, check NULL pointer for preferred_zoneref->zone. **CVE ID : CVE-2024-53113**		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Improve MSG_ZEROCOPY error handling Add a missing kfree_skb() to prevent memory leaks. **CVE ID : CVE-2024-53117**	https://git.kernel.org/stable/c/50061d7319e21165d04e3024354c1b43b6137821, https://git.kernel.org/stable/c/60cf6206a1f513512f5d73fa4d3dbbcad2e7dcd6	O-LIN-LINU-241224/1566
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix sk_error_queue memory leak Kernel queues MSG_ZEROCOPY completion	https://git.kernel.org/stable/c/bea4779a45f49275b1e1b1bd9de03cd3727244d8, https://git.kerne	O-LIN-LINU-241224/1567

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			notifications on the error queue. Where they remain, until explicitly recv()ed. To prevent memory leaks, clean up the queue when the socket is destroyed. unreferenced object 0xffff8881028beb00 (size 224): comm "vsock_test", pid 1218, jiffies 4294694897 hex dump (first 32 bytes): 90 b0 21 17 81 88 ff ff 90 b0 21 17 81 88 ff ff ..!.......!..... 00 00 00 00 00 00 00 00 00 b0 21 17 81 88 ff ff ....!..... backtrace (crc 6c7031ca): [<ffffffff81418ef7>] kmem_cache_alloc_node_noprof+0x2f7/0x370 [<ffffffff81d35882>] __alloc_skb+0x132/0x180 [<ffffffff81d2d32b>] sock_omalloc+0x4b/0x80 [<ffffffff81d3a8ae>] msg_zerocopy_realloc+0x9e/0x240 [<ffffffff81fe5cb2>] virtio_transport_send_pkt_info+0x412/0x4c0 [<ffffffff81fe6183>] virtio_transport_stream_enqueue+0x43/0x50	l.org/stable/c/fbf7085b3ad1c7cc0677834c90f985f1b4f77a33	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff81fe0813>] vsock_connectible_sendmsg+0x373/0x450 [<ffffffff81d233d5>] ____sys_sendmsg+0x365/0x3a0 [<ffffffff81d246f4>] ___sys_sendmsg+0x84/0xd0 [<ffffffff81d26f47>] __sys_sendmsg+0x47/0x80 [<ffffffff820d3df3>] do_syscall_64+0x93/0x180 [<ffffffff8220012b>] entry_SYSCALL_64_after_hwframe+0x76/0x7e **CVE ID : CVE-2024-53118**		
Missing Release of Memory after Effective Lifetime	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Fix accept_queue memory leak As the final stages of socket destruction may be delayed, it is possible that virtio_transport_recv_listen() will be called after the accept_queue has been flushed, but before the SOCK_DONE flag has been set. As a result, sockets enqueued after the flush would remain unremoved, leading to a memory leak.	https://git.kernel.org/stable/c/2415345042245de7601dcc6eafdbe3a3dcc9e379, https://git.kernel.org/stable/c/897617a413e0bf1c6380e3b34b2f28f450508549, https://git.kernel.org/stable/c/946c7600fa2207c	O-LIN-LINU-241224/1568

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_release __vsock_release lock virtio_transport_release virtio_transport_close schedule_delayed_work(close_work) sk_shutdown = SHUTDOWN_MASK (!) flush accept_queue release virtio_transport_recv_pkt vsock_find_bound_socket lock if flag(SOCK_DONE) return virtio_transport_recv_listen child = vsock_create_connected (!) vsock_enqueue_accept(child) release close_work lock virtio_transport_do_close set_flag(SOCK_DONE) virtio_transport_remove_sock vsock_remove_sock	c8d3fbc86a518ec56f98a5813	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vsock_remove_bound release Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction. unreferenced object 0xffff888109e3f800 (size 2040): comm "kworker/5:2", pid 371, jiffies 4294940105 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 (..@............ backtrace (crc 9e5f4e84): [<ffffffff81418ff1>] kmem_cache_alloc_noprof+0x2c1/0x360 [<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120 [<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0 [<ffffffff81fe049a>] __vsock_create.constprop.0+0x2a/0x310 [<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0x4dc/0x9a0 [<ffffffff81fe745d>] vsock_loopback_work+0xfd/0x140		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[<ffffffff810fc6ac>] process_one_work+0x20c/0x570 [<ffffffff810fce3f>] worker_thread+0x1bf/0x3a0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<ffffffff81044fdd>] ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0x30 **CVE ID : CVE-2024-53119**		
NULL Pointer Dereference	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr-deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule(), in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000110 RIP: 0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core]	https://git.kernel.org/stable/c/06dc488a593020bd2f006798557d2a32104d8359, https://git.kernel.org/stable/c/0c7c70ff8b696cfedba350411dca736361ef9a0f, https://git.kernel.org/stable/c/6030f8bd7902e9e276a0edc09bf11	O-LIN-LINU-241224/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			... Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0x30 ? mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] ? mlx5_tc_ct_entry_add_rule+0x1d5/0x2f0 [mlx5_core] mlx5_tc_ct_block_flow_offload+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] flow_offload_work_handler+0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x15b/0x2b0 process_one_work+0x16c/0x320	979e4e2bc2e	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			worker_thread+0x28c/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xb8/0xf0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> **CVE ID : CVE-2024-53120**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray.	https://git.kernel.org/stable/c/094d1a2121cee1e85ab07d74388f94809dcfb5b9, https://git.kernel.org/stable/c/933ef0d17f012b653e9e6006e3f50c8d0238b5ed, https://git.kernel.org/stable/c/9c	O-LIN-LINU-241224/1570

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely, causing a panic during subsequent rule deletions. To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to an FTE that is in the process of deletion. [438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func [438.968205] ------------[cut here]------------ [438.968654] refcount_t: decrement hit 0; leaking memory. [438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xfb/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch	a314419930f9135727e39d77e66262d5f7bef6	

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower] [438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [438.974874] RIP: 0010:refcount_warn_saturate+0xfb/0x110 [438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90 [438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286 [438.977446] RAX: 0000000000000000 RBX:		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ffff888119d56de0 RCX: 0000000000000000 [438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0 [438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0 [438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0 [438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0 [438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:0000000000000000 [438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 0000000000372eb0 [438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [438.985842] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [438.986507] Call Trace: [438.986799] <TASK>		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.987070] ? __warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xfb/0x110 [438.987877] ? report_bug+0x17d/0x190 [438.988261] ? prb_read_valid+0x17/0x20 [438.988659] ? handle_bug+0x53/0x90 [438.989054] ? exc_invalid_op+0x14/0x70 [438.989458] ? asm_exc_invalid_op+0x16/0x20 [438.989883] ? refcount_warn_saturate+0xfb/0x110 [438.990348] mlx5_del_flow_rules+0x2f7/0x340 [mlx5_core] [438.990932] __mlx5_eswitch_del_rule+0x49/0x170 [mlx5_core] [438.991519] ? mlx5_lag_is_sriov+0x3c/0x50 [mlx5_core] [438.992054] ? xas_load+0x9/0xb0 [438.992407] mlx5e_tc_rule_unoffload+0x45/0xe0 [mlx5_core] [438.993037] mlx5e_tc_del_fdb_flow+0x2a6/0x2e0 [mlx5_core] [438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core]		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			[438.994161] mlx5e_delete_flower+0x261/0x390 [mlx5_core] [438.994728] tc_setup_cb_destroy+0xb9/0x190 [438.995150] fl_hw_destroy_filter+0x94/0xc0 [cls_flower] [438.995650] fl_change+0x11a4/0x13c0 [cls_flower] [438.996105] tc_new_tfilter+0x347/0xbc0 [438.996503] ? __ ---truncated--- **CVE ID : CVE-2024-53121**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: cope racing subflow creation in mptcp_rcv_space_adjust Additional active subflows - i.e. created by the in kernel path manager - are included into the subflow list before starting the 3whs. A racing recvmsg() spooling data received on an already established subflow would unconditionally call	https://git.kernel.org/stable/c/24995851d58c4a205ad0ffa7b2f21e479a9c8527, https://git.kernel.org/stable/c/aad6412c63baa39dd813e81f16a14d976b3de2e8, https://git.kernel.org/stable/c/ce	O-LIN-LINU-241224/1571

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf(). **CVE ID : CVE-2024-53122**	7356ae35943cc6494cc692e62d51a734062b7d	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024	https://git.kernel.org/stable/c/581302298524e9d77c4c44ff5156a6cd112227ae, https://git.kernel.org/stable/c/955388e1d5d222c4101c596b536d41b91a8b212e, https://git.kernel.org/stable/c/a66805c9b22caf4e42af7a616f6c6b	O-LIN-LINU-241224/1572

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RIP: 0010:__tcp_select_window+0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80 R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033	83c90d1010	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289 inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline] __se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:52 [inline]		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			do_syscall_64+0xcd/0x250 arch/x86/entry/common.c: 83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559 RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000fffffdef and provided a nice reproducer.		

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss. Catch the error and return without performing any additional operations on the current socket. **CVE ID : CVE-2024-53123**		
Always-Incorrect Control Flow Implementation	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: correct remove path The check condition should be 'i < bc->onecell_data.num_domains', not 'bc->onecell_data.num_domains' which will make the look never finish and cause kernel panic. Also disable runtime to address "imx93-blk-ctrl 4ac10000.system-	https://git.kernel.org/stable/c/201fb9e164a1e4c5937de2cf58bcb0327c08664f, https://git.kernel.org/stable/c/8fc228ab5d38a026eae7183a5f74a4fac43d9b6a, https://git.kernel.org/stable/c/f7c7c5aa556378a2	O-LIN-LINU-241224/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			controller: Unbalanced pm_runtime_enable!" **CVE ID : CVE-2024-53134**	c8da72c1f7f238b6648f95fb	
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resync_dump_comp()), only put_page() is used. This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc() references are stored directly in the given page. On release the folio page will be dereferenced too many times. This was found while doing kTLS testing with sendfile() + ZC when the	https://git.kernel.org/stable/c/2723e8b2cbd486cb96e5a61b22473f7fd62e18df, https://git.kernel.org/stable/c/69fbd07f17b0fdaf8970bc705f5bf115c297839d, https://git.kernel.org/stable/c/93a14620b97c911489a5b008782f3d9b0c4aeff4	O-LIN-LINU-241224/1574

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
			served file was read from NFS on a kernel with NFS large folios support (commit 49b29a573da8 ("nfs: add support for large folios")). **CVE ID : CVE-2024-53138**		
N/A	04-Dec-2024	5.5	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket.	https://git.kernel.org/stable/c/114a61d8d94ae3a43b82446cf737fd757021b834, https://git.kernel.org/stable/c/176c41b3ca9281a9736b67c6121b03dbf0c8c08f, https://git.kernel.org/stable/c/1904fb9ebf911441f90a68e96b22aa73e4410505	O-LIN-LINU-241224/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone else holds the socket they may release it in BH and we're back to square one. The whole dance, however, appears to be unnecessary. Only the user		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own. **CVE ID : CVE-2024-53140**		
Affected Version(s): From (including) 6.7 Up to (excluding) 6.11.11					
N/A	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists,	https://git.kernel.org/stable/c/15794835378ed56fb9bacc6a5dd3b9f33520604e, https://git.kernel.org/stable/c/3	O-LIN-LINU-241224/1576

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE ID : CVE-2024-53141**	5f56c554eb1b56b77b3cf197a6b00922d49033d, https://git.kernel.org/stable/c/3c20b5948f119ae61ee35ad8584d666020c91581	
Out-of-bounds Write	06-Dec-2024	7.8	In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in Documentation/driver-api/early-userspace/buffer-format.rst as: 37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data ... 55 ============= ================== ===================== ==== 56 Field name Field size Meaning	https://git.kernel.org/stable/c/1a423bbbeaf9e3e20c4686501efd9b661fe834db, https://git.kernel.org/stable/c/49d01e736c3045319e030d1e75fb983011abaca7, https://git.kernel.org/stable/c/bb7ac96670ab1d8d681015f9d66e45	O-LIN-LINU-241224/1577

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
		🟧	57 === ... 70 c_namesize 8 bytes Length of filename, including final \0 When extracting an initramfs cpio archive, the kernel's do_name() path handler assumes a zero-terminated path at @collected, passing it directly to filp_open() / init_mkdir() / init_mknod(). If a specially crafted cpio entry carries a non-zero-terminated filename and is followed by uninitialized memory, then a file may be created with trailing characters that represent the uninitialized memory. The ability to create an initramfs entry would imply already having full control of the system, so the buffer overrun shouldn't be considered a security vulnerability. Append the output of the following bash script to an existing initramfs	dad579af4d	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID

		🟧	and observe any created /initramfs_test_fname_overrunAA* path. E.g.
			./reproducer.sh | gzip >> /myinitramfs
			It's easiest to observe non-zero uninitialized memory when the output is
			gzipped, as it'll overflow the heap allocated @out_buf in __gunzip(),
			rather than the initrd_start+initrd_size block.
			---- reproducer.sh ----
			nilchar="A" # change to "\0" to properly zero terminate / pad
			magic="070701"
			ino=1
			mode=$((0100777))
			uid=0
			gid=0
			nlink=1
			mtime=1
			filesize=0
			devmajor=0
			devminor=1
			rdevmajor=0
			rdevminor=0
			csum=0
			fname="initramfs_test_fname_overrun"		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			namelen=$((${#fname} + 1)) # plus one to account for terminator printf "%s%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%s" \ $magic $ino $mode $uid $gid $nlink $mtime $filesize \ $devmajor $devminor $rdevmajor $rdevminor $namelen $csum $fname termpadlen=$((1 + ((4 - ((110 + $namelen) & 3)) % 4))) printf "%.s${nilchar}" $(seq 1 $termpadlen) ---- reproducer.sh ---- Symlink filename fields handled in do_symlink() won't overrun past the data segment, due to the explicit zero-termination of the symlink target. Fix filename buffer overrun by aborting the initramfs FSM if any cpio entry doesn't carry a zero-terminator at the expected (name_len - 1)		

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			offset. **CVE ID : CVE-2024-53142**		
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Integer Underflow (Wrap or Wraparound)	10-Dec-2024	7.8	Bridge versions 14.1.3, 15.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53955**	https://helpx.adobe.com/security/products/bridge/apsb24-103.html	O-MIC-WIND-241224/1578
Heap-based Buffer Overflow	10-Dec-2024	7.8	Premiere Pro versions 25.0, 24.6.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2024-53956**	https://helpx.adobe.com/security/products/premiere_pro/apsb24-104.html	O-MIC-WIND-241224/1579
Stack-based Buffer Overflow	10-Dec-2024	7.8	Adobe Framemaker versions 2020.7, 2022.5 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in	https://helpx.adobe.com/security/products/framemaker/apsb24-	O-MIC-WIND-241224/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that a victim must open a malicious file. **CVE ID : CVE-2024-53959**	106.html	
Product: windows_10_1507					
Affected Version(s): * Up to (excluding) 10.0.10240.20857					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1581
Product: windows_10_1607					
Affected Version(s): * Up to (excluding) 10.0.14393.7606					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1582
Product: windows_10_1809					
Affected Version(s): * Up to (excluding) 10.0.17763.6659					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1583
Product: windows_10_21h2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 10.0.19044.5247					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1584
Product: windows_10_22h2					
Affected Version(s): * Up to (excluding) 10.0.19045.5247					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1585
Product: windows_11_22h2					
Affected Version(s): * Up to (excluding) 10.0.22621.4602					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1586
Product: windows_11_23h2					
Affected Version(s): * Up to (excluding) 10.0.22631.4602					
Heap-based	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability	https://msrc.microsoft.c	O-MIC-WIND-241224/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			**CVE ID : CVE-2024-49138**	om/update-guide/vulnerability/CVE-2024-49138	
Product: windows_11_24h2					
Affected Version(s): * Up to (excluding) 10.0.26100.2605					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1588
Product: windows_server_2008					
Affected Version(s): -					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1589
Affected Version(s): r2					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE	O-MIC-WIND-241224/1590

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				-2024-49138	
Affected Version(s): sp2					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1591
Product: windows_server_2012					
Affected Version(s): -					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1592
Affected Version(s): r2					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1593
Product: windows_server_2016					
Affected Version(s): * Up to (excluding) 10.0.14393.7606					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1594
Product: windows_server_2019					
Affected Version(s): * Up to (excluding) 10.0.17763.6659					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1595
Product: windows_server_2022					
Affected Version(s): * Up to (excluding) 10.0.20348.2966					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1596
Product: windows_server_2022_23h2					
Affected Version(s): * Up to (excluding) 10.0.25398.1308					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-	O-MIC-WIND-241224/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				guide/vulnerability/CVE-2024-49138	
Product: windows_server_2025					
Affected Version(s): * Up to (excluding) 10.0.26100.2605					
Heap-based Buffer Overflow	12-Dec-2024	7.8	Windows Common Log File System Driver Elevation of Privilege Vulnerability **CVE ID : CVE-2024-49138**	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138	O-MIC-WIND-241224/1598
Vendor: openatom					
Product: openharmony					
Affected Version(s): * Up to (including) 4.0					
Out-of-bounds Read	03-Dec-2024	5.5	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause information leak through out-of-bounds Read. **CVE ID : CVE-2024-12082**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-12.md	O-OPE-OPEN-241224/1599
Affected Version(s): * Up to (including) 4.1.1					
Use After Free	03-Dec-2024	8.8	in OpenHarmony v4.1.1 and prior versions allow a local attacker cause the common permission is upgraded to root through use after free. **CVE ID : CVE-2024-10074**	https://gitee.com/openharmony/security/blob/master/	O-OPE-OPEN-241224/1600

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				zh/security-disclosure/2024/2024-12.md	
Out-of-bounds Read	03-Dec-2024	5.5	in OpenHarmony v4.1.1 and prior versions allow a local attacker cause information leak through out-of-bounds Read. **CVE ID : CVE-2024-9978**	https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2024/2024-12.md	O-OPE-OPEN-241224/1601
Vendor: Qualcomm					
Product: 205_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-205_-241224/1602
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-205_-241224/1603

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: 215_mobile_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-215_-241224/1604
Product: 315_5g_iot_modem_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-315_-241224/1605
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/pu	O-QUA-315_-241224/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Product: 9205_lte_modem_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-9205-241224/1607
Product: 9206_lte_modem_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-9206-241224/1608
Product: 9207_lte_modem_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-9207-241224/1609
Product: apq8017_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-APQ8-241224/1610
Product: apq8037_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-APQ8-241224/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: aqt1000_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-AQT1-241224/1612
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-AQT1-241224/1613
Product: ar8035_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-AR80-241224/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-AR80-241224/1615
Product: c-v2x_9150_firmware					
Affected Version(s): -					
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-C-V2-241224/1616
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de cember-	O-QUA-C-V2-241224/1617

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-C-V2-241224/1618
Product: csrb31024_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-CSRB-241224/1619
Product: fastconnect_6200_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-FAST-241224/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1621
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1622
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-FAST-241224/1623

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1624
Product: fastconnect_6700_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1625
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-FAST-241224/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1627
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1628
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1629
Product: fastconnect_6800_firmware					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1630
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1631
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1633
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1634
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1635
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	O-QUA-FAST-241224/1636

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1637
Product: fastconnect_6900_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1638
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	O-QUA-FAST-241224/1639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1640
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1641
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-FAST-241224/1642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1643
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1644
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1645

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1646
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1647
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1648
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-FAST-241224/1649

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: fastconnect_7800_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1650
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1651
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	O-QUA-FAST-241224/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1653
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1654
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-FAST-241224/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1656
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1657
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FAST-241224/1659
Product: flight_rb5_5g_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FLIG-241224/1660
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FLIG-241224/1661
Product: fsm10055_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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FSM1-241224/1662
Product: fsm10056_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-FSM1-241224/1663
Product: home_hub_100_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-HOME-241224/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-HOME-241224/1665
Product: immersive_home_214_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IMME-241224/1666
Product: immersive_home_216_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-IMME-241224/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: immersive_home_316_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IMME-241224/1668
Product: immersive_home_318_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IMME-241224/1669
Product: immersive_home_3210_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/pro	O-QUA-IMME-241224/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IMME-241224/1671
Product: immersive_home_326_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IMME-241224/1672
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-IMME-241224/1673

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: ipq5010_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1674
Product: ipq5028_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1675
Product: ipq5300_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1676
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1677
Product: ipq5302_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1678
Product: ipq5312_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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1679
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1680
Product: ipq5332_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1681

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ5-241224/1682
Product: ipq6000_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ6-241224/1683
Product: ipq6005_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-IPQ6-241224/1684

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: ipq6010_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ6-241224/1685
Product: ipq6018_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ6-241224/1686
Product: ipq6028_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-IPQ6-241224/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: ipq8064_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1688
Product: ipq8065_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1689
Product: ipq8068_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	O-QUA-IPQ8-241224/1690

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: ipq8070a_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1691
Product: ipq8070_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1692
Product: ipq8071a_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1693
Product: ipq8071_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1694
Product: ipq8072a_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-IPQ8-241224/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: ipq8072_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1696
Product: ipq8074a_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1697
Product: ipq8074_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	O-QUA-IPQ8-241224/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: ipq8076a_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1699
Product: ipq8076_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1700
Product: ipq8078a_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1701
Product: ipq8078_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1702
Product: ipq8173_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-IPQ8-241224/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: ipq8174_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ8-241224/1704
Product: ipq9008_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ9-241224/1705
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-IPQ9-241224/1706

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: ipq9554_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ9-241224/1707
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ9-241224/1708
Product: ipq9570_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-IPQ9-241224/1709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ9-241224/1710
Product: ipq9574_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-IPQ9-241224/1711
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-IPQ9-241224/1712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: mdm8207_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MDM8-241224/1713
Product: mdm9205s_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MDM9-241224/1714
Product: mdm9250_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.com/pro	O-QUA-MDM9-241224/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: mdm9628_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MDM9-241224/1716
Product: mdm9650_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MDM9-241224/1717
Product: msm8108_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1718
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1719
Product: msm8209_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1720

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1721
Product: msm8608_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1722
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1723
Product: msm8909w_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-MSM8-241224/1724
Product: pm8937_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-PM89-241224/1725
Product: pmp8074_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-PMP8-241224/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: qam8255p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1727
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1728
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QAM8-241224/1729

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1730
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1731
Product: qam8295p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QAM8-241224/1732

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1733
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1734
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1735

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1736
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1737
Product: qam8620p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1738

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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1739
Product: qam8650p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1740
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1741

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1742
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1743
Product: qam8775p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1745
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1746
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAM8-241224/1747
Product: qamsrv1h_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1748
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1749
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1750
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	O-QUA-QAMS-241224/1751

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qamsrv1m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1752
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1753
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-QAMS-241224/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QAMS-241224/1755
Product: qca0000_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA0-241224/1756
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso	O-QUA-QCA0-241224/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: qca1062_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA1-241224/1758
Product: qca1064_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA1-241224/1759
Product: qca2062_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1760
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1761
Product: qca2064_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1763
Product: qca2065_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1764
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1765
Product: qca2066_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1766
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA2-241224/1767
Product: qca4004_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA4-241224/1768

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qca4024_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA4-241224/1769
Product: qca6164_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1770
Product: qca6174a_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCA6-241224/1771

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1772
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1773
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1775
Product: qca6174_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1776
Product: qca6310_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCA6-241224/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1778
Product: qca6320_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1779
Product: qca6335_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCA6-241224/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1781
Product: qca6391_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1782
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-cember-	O-QUA-QCA6-241224/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1784
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1785
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1786

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1787
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1788
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1789
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-QCA6-241224/1790

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6420_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1791
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1792
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https://docs.qualcomm.com/product/pu	O-QUA-QCA6-241224/1793

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43050	blicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6421_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1794
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1795
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicreso	O-QUA-QCA6-241224/1796

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: qca6426_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1797
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1798
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCA6-241224/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1800
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1801
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCA6-241224/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1803
Product: qca6428_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1804
Product: qca6430_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCA6-241224/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1806
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1807
Product: qca6431_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-QCA6-241224/1808

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1809
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1810
Product: qca6436_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCA6-241224/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1812
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1813
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1815
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1816
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1817
Product: qca6438_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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1818
Product: qca6554a_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1819
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1820
Product: qca6564au_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1821
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1822
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1823
Product: qca6564a_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1824
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1825
Product: qca6564_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1826

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1827
Product: qca6574au_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1828
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1829

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1830
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1831
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1832
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-QCA6-241224/1833

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6574a_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1834
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1835
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-QCA6-241224/1836

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6574_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1837
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1838
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso	O-QUA-QCA6-241224/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: qca6584au_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1840
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1841
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso urces/se	O-QUA-QCA6-241224/1842

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	curitybulletin/december-2024-bulletin.html	
Product: qca6595au_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1843
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1844
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin	O-QUA-QCA6-241224/1845

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1846
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1847
Product: qca6595_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCA6-241224/1848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1849
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1850
Product: qca6678aq_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-QCA6-241224/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1852
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1853
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qca6688aq_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1855
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1856
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1857
Product: qca6694_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1858
Product: qca6696_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1859
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1860

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1861
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1862
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1863
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-QCA6-241224/1864

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6698aq_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1865
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1866
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-QCA6-241224/1867

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: qca6777aq_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1868
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1869
Product: qca6787aq_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	O-QUA-QCA6-241224/1870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1871
Product: qca6797aq_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1872
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	O-QUA-QCA6-241224/1873

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA6-241224/1874
Product: qca8072_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1875
Product: qca8075_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qua	O-QUA-QCA8-241224/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1877
Product: qca8081_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1878
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	O-QUA-QCA8-241224/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1880
Product: qca8082_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1881
Product: qca8084_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1882
Product: qca8085_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1883
Product: qca8337_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCA8-241224/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1885
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1886
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1888
Product: qca8386_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA8-241224/1889
Product: qca9377_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCA9-241224/1890

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA9-241224/1891
Product: qca9379_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCA9-241224/1892
Product: qcc2073_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCC2-241224/1893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCC2-241224/1894
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCC2-241224/1895
Product: qcc2076_firmware					
Affected Version(s): -					
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-QCC2-241224/1896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCC2-241224/1897
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCC2-241224/1898
Product: qcc710_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCC7-241224/1899

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCC7-241224/1900
Product: qcf8000_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCF8-241224/1901
Product: qcf8001_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCF8-241224/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: qcm2150_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM2-241224/1903
Product: qcm4325_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM4-241224/1904
Product: qcm5430_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	O-QUA-QCM5-241224/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM5-241224/1906
Product: qcm6490_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM6-241224/1907
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https://docs.qualcomm.com/product/publicreso	O-QUA-QCM6-241224/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43050	urces/securitybulletin/december-2024-bulletin.html	
Product: qcm8550_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM8-241224/1909
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM8-241224/1910
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCM8-241224/1911

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCM8-241224/1912
Product: qcn5124_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN5-241224/1913
Product: qcn6224_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	O-QUA-QCN6-241224/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1915
Product: qcn6274_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1916
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicresources	O-QUA-QCN6-241224/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: qcn6402_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1918
Product: qcn6412_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1919
Product: qcn6422_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1920
Product: qcn6432_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN6-241224/1921
Product: qcn7605_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCN7-241224/1922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qcn7606_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN7-241224/1923
Product: qcn9000_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1924
Product: qcn9011_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCN9-241224/1925

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: qcn9012_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1926
Product: qcn9024_firmware					
Affected Version(s): -					
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1927
Product: qcn9074_firmware					
Affected Version(s): -					
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info	https://docs.qualcomm.c	O-QUA-QCN9-241224/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1929
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1930
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCN9-241224/1931

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33037	curitybulletin/december-2024-bulletin.html	
Product: qcn9160_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1932
Product: qcn9274_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1933
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/pu	O-QUA-QCN9-241224/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1935
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCN9-241224/1936
Product: qcs2290_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	O-QUA-QCS2-241224/1937

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: qcs410_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS4-241224/1938
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS4-241224/1939
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCS4-241224/1940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS4-241224/1941
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS4-241224/1942
Product: qcs4290_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-QCS4-241224/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: qcs4490_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS4-241224/1944
Product: qcs5430_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS5-241224/1945
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	O-QUA-QCS5-241224/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS5-241224/1947
Product: qcs610_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1948
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-QCS6-241224/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1950
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCS6-241224/1951
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCS6-241224/1952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: qcs6125_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1953
Product: qcs6490_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1954
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-QCS6-241224/1955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1956
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS6-241224/1957
Product: qcs7230_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-QCS7-241224/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS7-241224/1959
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS7-241224/1960
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS7-241224/1961

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: qcs8155_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1962
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1963
Product: qcs8250_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QCS8-241224/1964

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1965
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1966
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1967
Product: qcs8550_firmware					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1968
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1969
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS8-241224/1970
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https://docs.qua	O-QUA-QCS8-241224/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qcs9100_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS9-241224/1972
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QCS9-241224/1973
Product: qdu1000_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1974
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1975
Product: qdu1010_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1977
Product: qdu1110_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1978
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1979
Product: qdu1210_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1980
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDU1-241224/1981
Product: qdx1010_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDX1-241224/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDX1-241224/1983
Product: qdx1011_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDX1-241224/1984
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QDX1-241224/1985
Product: qep8111_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QEP8-241224/1986
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QEP8-241224/1987
Product: qet4101_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QET4-241224/1988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: qfw7114_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1989
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1990
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1991
Product: qfw7124_firmware					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1992
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1993
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QFW7-241224/1994
Product: qrb5165m_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRB5-241224/1995
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRB5-241224/1996
Product: qrb5165n_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRB5-241224/1997

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRB5-241224/1998
Product: qru1032_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/1999
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/2000
Product: qru1052_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/2001
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/2002
Product: qru1062_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/2003

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QRU1-241224/2004
Product: qsm8250_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2005
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2007
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2008
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2009
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-QSM8-241224/2010

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: qsm8350_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2011
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSM8-241224/2012
Product: qsw8573_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QSW8-241224/2013
Product: qts110_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-QTS1-241224/2014
Product: qxm8083_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-QXM8-241224/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: robotics_rb3_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-ROBO-241224/2016
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-ROBO-241224/2017
Product: robotics_rb5_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-ROBO-241224/2018

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-ROBO-241224/2019
Product: sa2150p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA21-241224/2020
Product: sa4150p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SA41-241224/2021

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA41-241224/2022
Product: sa4155p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA41-241224/2023
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-SA41-241224/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: sa6145p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2025
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2026
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SA61-241224/2027

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33036	cember-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2028
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2029
Product: sa6150p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SA61-241224/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2031
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2032
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2033

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2034
Product: sa6155p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2035
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2037
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2038
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2039
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-SA61-241224/2040

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa6155_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2041
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA61-241224/2042
Product: sa7255p_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA72-241224/2043
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA72-241224/2044
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA72-241224/2045
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	O-QUA-SA72-241224/2046

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa7775p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA77-241224/2047
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA77-241224/2048
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-SA77-241224/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA77-241224/2050
Product: sa8145p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2051
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	O-QUA-SA81-241224/2052

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2053
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2054
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SA81-241224/2055

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: sa8150p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2056
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2057
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SA81-241224/2058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2059
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2060
Product: sa8155p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SA81-241224/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2062
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2063
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2065
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2066
Product: sa8155_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2068
Product: sa8195p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2069
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2071
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2072
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA81-241224/2073
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t	https://docs.qualcomm.com/pro	O-QUA-SA81-241224/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa8255p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2075
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2076
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-SA82-241224/2077

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2078
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2079
Product: sa8295p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	O-QUA-SA82-241224/2080

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2081
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2082
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SA82-241224/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2084
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA82-241224/2085
Product: sa8530p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SA85-241224/2086

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2087
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2088
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2089

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2090
Product: sa8540p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2091
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2093
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2094
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA85-241224/2095
Product: sa8620p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2096
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2097
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2098
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	O-QUA-SA86-241224/2099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sa8650p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2100
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2101
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-SA86-241224/2102

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA86-241224/2103
Product: sa8770p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA87-241224/2104
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources	O-QUA-SA87-241224/2105

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA87-241224/2106
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA87-241224/2107
Product: sa8775p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SA87-241224/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA87-241224/2109
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA87-241224/2110
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SA87-241224/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sa9000p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2112
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2113
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SA90-241224/2114

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2115
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2116
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2117

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SA90-241224/2118
Product: sc8180x_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC81-241224/2119
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC81-241224/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC81-241224/2121
Product: sc8380xp_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC83-241224/2122
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC83-241224/2123

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC83-241224/2124
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC83-241224/2125
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SC83-241224/2126
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https://docs.qualcomm.com/pro	O-QUA-SC83-241224/2127

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. **CVE ID : CVE-2024-43053**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sd460_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD46-241224/2128
Product: sd660_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD66-241224/2129
Product: sd662_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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD66-241224/2130
Product: sd670_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD67-241224/2131
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD67-241224/2132
Product: sd675_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD67-241224/2133
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD67-241224/2134
Product: sd730_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD73-241224/2135

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD73-241224/2136
Product: sd835_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD83-241224/2137
Product: sd855_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SD85-241224/2138

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD85-241224/2139
Product: sd865_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2140
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SD86-241224/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2142
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2143
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2144

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2145
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD86-241224/2146
Product: sd888_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD88-241224/2147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD88-241224/2148
Product: sdm429w_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2149
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2150

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2151
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2152
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2153
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https://docs.qualcomm.com/pro	O-QUA-SDM4-241224/2154

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2155
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDM4-241224/2156
Product: sdx20m_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	O-QUA-SDX2-241224/2157

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Product: sdx55_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2158
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2159
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	https://docs.qualcomm.com/product/publicreso	O-QUA-SDX5-241224/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43050	urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2161
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2162
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SDX5-241224/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2164
Product: sdx57m_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX5-241224/2165
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SDX5-241224/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: sdx61_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX6-241224/2167
Product: sdx65m_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX6-241224/2168
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SDX6-241224/2169

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: sdx71m_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SDX7-241224/2170
Product: sd_455_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_4-241224/2171
Product: sd_675_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	O-QUA-SD_6-241224/2172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_6-241224/2173
Product: sd_8cx_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_8-241224/2174
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_8-241224/2175

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: sd_8_gen1_5g_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_8-241224/2176
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SD_8-241224/2177
Product: sg4150p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	O-QUA-SG41-241224/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SG41-241224/2179
Product: sg8275p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SG82-241224/2180
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	O-QUA-SG82-241224/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SG82-241224/2182
Product: sm4125_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM41-241224/2183
Product: sm4635_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qualcomm.c	O-QUA-SM46-241224/2184

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM46-241224/2185
Product: sm6250p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM62-241224/2186
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	O-QUA-SM62-241224/2187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm6250_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM62-241224/2188
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM62-241224/2189
Product: sm6370_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an	https://docs.qua	O-QUA-SM63-241224/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm7250p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM72-241224/2191
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM72-241224/2192
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to	https://docs.qualcomm.c	O-QUA-SM72-241224/2193

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm7315_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM73-241224/2194
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM73-241224/2195
Product: sm7325p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM73-241224/2196
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM73-241224/2197
Product: sm8550p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM85-241224/2198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM85-241224/2199
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM85-241224/2200
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM85-241224/2201
Product: sm8635_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM86-241224/2202
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM86-241224/2203
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM86-241224/2204
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/pro	O-QUA-SM86-241224/2205

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: sm8750p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2206
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2207
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	O-QUA-SM87-241224/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2209
Product: sm8750_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2210
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicreso	O-QUA-SM87-241224/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2212
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SM87-241224/2213
Product: smart_audio_200_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SMAR-241224/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SMAR-241224/2215
Product: smart_audio_400_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SMAR-241224/2216
Product: snapdragon_1100_wearable_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/pu	O-QUA-SNAP-241224/2217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_1200_wearable_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2218
Product: snapdragon_208_processor_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2219
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https://docs.qualcomm.c	O-QUA-SNAP-241224/2220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_210_processor_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2221
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2222
Product: snapdragon_212_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2223
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2224
Product: snapdragon_425_mobile_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2225
Product: snapdragon_427_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2226
Product: snapdragon_429_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2227
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2229
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2230
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2231
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https://docs.qualcomm.com/pro	O-QUA-SNAP-241224/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43052	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2233
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2234
Product: snapdragon_430_mobile_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	O-QUA-SNAP-241224/2235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_435_mobile_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2236
Product: snapdragon_439_mobile_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2237
Product: snapdragon_460_mobile_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2238
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2239
Product: snapdragon_480\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2241
Product: snapdragon_480_5g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2242
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2243
Product: snapdragon_4_gen_1_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2244
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2245
Product: snapdragon_4_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2246

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_630_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2247
Product: snapdragon_636_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2248
Product: snapdragon_660_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: snapdragon_662_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2250
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2251
Product: snapdragon_665_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SNAP-241224/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Product: snapdragon_670_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2253
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2254
Product: snapdragon_675_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	O-QUA-SNAP-241224/2255

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2256
Product: snapdragon_678_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2257
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	O-QUA-SNAP-241224/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_680_4g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2259
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2260
Product: snapdragon_685_4g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/pro	O-QUA-SNAP-241224/2261

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2262
Product: snapdragon_690_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2263
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	O-QUA-SNAP-241224/2264

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2265
Product: snapdragon_695_5g_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2266
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/	O-QUA-SNAP-241224/2267

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Product: snapdragon_710_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2268
Product: snapdragon_712_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2269
Product: snapdragon_720g_mobile_platform_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2270
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2271
Product: snapdragon_730g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2273
Product: snapdragon_730_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2274
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2275
Product: snapdragon_732g_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2276
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2277
Product: snapdragon_750g_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2278

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2279
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2280
Product: snapdragon_765g_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2281

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2282
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2283
Product: snapdragon_765_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2285
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2286
Product: snapdragon_768g_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2287

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2288
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2289
Product: snapdragon_778g\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2291
Product: snapdragon_778g_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2292
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2293
Product: snapdragon_780g_5g_mobile_platform_firmware					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2294
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2295
Product: snapdragon_782g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2297
Product: snapdragon_7c\+_gen_3_compute_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2298
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2300
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2301
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2302
Product: snapdragon_7c_compute_platform_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2303
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2304
Product: snapdragon_7c_gen_2_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2306
Product: snapdragon_820_automotive_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2307
Product: snapdragon_835_mobile_pc_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_845_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2309
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2310
Product: snapdragon_850_mobile_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2311

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2312
Product: snapdragon_855\+_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2313
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SNAP-241224/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: snapdragon_855_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2315
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2316
Product: snapdragon_860_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-SNAP-241224/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2318
Product: snapdragon_865\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2319
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2321
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2322
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2323

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2324
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2325
Product: snapdragon_865_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2326

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2327
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2328
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2329
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	O-QUA-SNAP-241224/2330

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2331
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2332
Product: snapdragon_870_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/pu	O-QUA-SNAP-241224/2333

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2334
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2335
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33036	cember-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2337
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2338
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2339

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: snapdragon_888\+_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2340
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2341
Product: snapdragon_888_5g_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2343
Product: snapdragon_8cx_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2344
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2346
Product: snapdragon_8cx_gen_2_5g_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2347
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2348

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2349
Product: snapdragon_8cx_gen_3_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2350
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2352
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2353
Product: snapdragon_8c_compute_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2354

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2355
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2356
Product: snapdragon_8\+_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_8\+_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2358
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2359
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2360

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2361
Product: snapdragon_8_gen_1_mobile_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2362
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2363

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2364
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2365
Product: snapdragon_8_gen_2_mobile_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2367
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2368
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2369
Product: snapdragon_8_gen_3_mobile_platform_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2370
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2371
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2372

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2373
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2374
Product: snapdragon_ar2_gen_1_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2375

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2376
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2377
Product: snapdragon_auto_4g_modem_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2378

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2379
Product: snapdragon_auto_5g_modem-rf_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2380
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2381
Product: snapdragon_auto_5g_modem-rf_gen_2_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2382
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2383
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2384
Product: snapdragon_w5\+_gen_1_wearable_platform_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2385
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2386
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2387
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	O-QUA-SNAP-241224/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2389
Product: snapdragon_wear_1300_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2390
Product: snapdragon_wear_2100_platform_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2391
Product: snapdragon_wear_2500_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2392
Product: snapdragon_wear_3100_platform_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2393

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_wear_4100\+_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2394
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2395
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_x12_lte_modem_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2397
Product: snapdragon_x20_lte_modem_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2398
Product: snapdragon_x24_lte_modem_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SNAP-241224/2399

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2400
Product: snapdragon_x35_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2401
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin	O-QUA-SNAP-241224/2402

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: snapdragon_x50_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2403
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2404
Product: snapdragon_x55_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	O-QUA-SNAP-241224/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2406
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2407
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SNAP-241224/2408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2409
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2410
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2411

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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_x5_lte_modem_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2412
Product: snapdragon_x62_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2413
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_x65_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2415
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2416
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SNAP-241224/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: snapdragon_x70_modem-rf_system_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2418
Product: snapdragon_x72_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2419
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2420

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2421
Product: snapdragon_x75_5g_modem-rf_system_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2422
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SNAP-241224/2423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2424
Product: snapdragon_xr1_platform_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2425
Product: snapdragon_xr2\+_gen_1_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-SNAP-241224/2426

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2427
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2428
Product: snapdragon_xr2_5g_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SNAP-241224/2429

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2430
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2431
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2432

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2433
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2434
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SNAP-241224/2435
Product: srv1h_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2436
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2437
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2438
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	O-QUA-SRV1-241224/2439

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: srv1l_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2440
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2441
Product: srv1m_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2442
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2443
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SRV1-241224/2444
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the	https://docs.qualcomm.com/pro	O-QUA-SRV1-241224/2445

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle is not validated by the service. **CVE ID : CVE-2024-33039**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Product: ssg2115p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SSG2-241224/2446
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SSG2-241224/2447
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/product/pu	O-QUA-SSG2-241224/2448

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	blicresources/securitybulletin/december-2024-bulletin.html	
Product: ssg2125p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SSG2-241224/2449
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SSG2-241224/2450
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	https://docs.qualcomm.com/product/publicreso	O-QUA-SSG2-241224/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33063	urces/securitybulletin/december-2024-bulletin.html	
Product: sw5100p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2452
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2453
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	https://docs.qualcomm.com/product/publicresources/se	O-QUA-SW51-241224/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33039	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2455
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2456
Product: sw5100_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-SW51-241224/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2458
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2459
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-SW51-241224/2460

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SW51-241224/2461
Product: sxr1120_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR1-241224/2462
Product: sxr1230p_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-SXR1-241224/2463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR1-241224/2464
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR1-241224/2465
Product: sxr2130_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-SXR2-241224/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2467
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2468
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2470
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2471
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2472
Product: sxr2230p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2473
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2474
Product: sxr2250p_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2475

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-SXR2-241224/2476
Product: talynplus_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-TALY-241224/2477
Product: video_collaboration_vc1_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-VIDE-241224/2478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2479
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2480
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2481

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2482
Product: video_collaboration_vc3_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2483
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2485
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2486
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2487
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	O-QUA-VIDE-241224/2488

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2489
Product: video_collaboration_vc5_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2490
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	https://docs.qualcomm.com/product/pu	O-QUA-VIDE-241224/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33056	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2492
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VIDE-241224/2493
Product: vision_intelligence_300_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	O-QUA-VISI-241224/2494

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VISI-241224/2495
Product: vision_intelligence_400_platform_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VISI-241224/2496
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-VISI-241224/2497

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VISI-241224/2498
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-VISI-241224/2499
Product: wcd9306_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WCD9-241224/2500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcd9326_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2501
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2502
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-WCD9-241224/2503

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Product: wcd9330_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2504
Product: wcd9335_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2505
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-WCD9-241224/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2507
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2508
Product: wcd9340_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin	O-QUA-WCD9-241224/2509

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2510
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2511
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCD9-241224/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wcd9341_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2513
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2514
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCD9-241224/2515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2516
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2517
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2518

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2519
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2520
Product: wcd9360_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2521

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2522
Product: wcd9370_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2523
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2524

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2525
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2526
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2527
Integer Overflow or	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater	https://docs.qualcomm.com/pro	O-QUA-WCD9-241224/2528

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Wraparound			than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2529
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2530
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WCD9-241224/2531

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcd9371_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2532
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2533
Product: wcd9375_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicreso	O-QUA-WCD9-241224/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2535
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2536
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-WCD9-241224/2537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2538
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2539
Product: wcd9378_firmware					
Affected Version(s): -					
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCD9-241224/2540

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wcd9380_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2541
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2542
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCD9-241224/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2544
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2545
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2547
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2548
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2549
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	https://docs.qualcomm.com/pro	O-QUA-WCD9-241224/2550

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-33053	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2551
Product: wcd9385_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2552
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	O-QUA-WCD9-241224/2553

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2554
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2555
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-WCD9-241224/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2557
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2558
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2559

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wcd9390_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2560
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2561
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2562

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2563
Product: wcd9395_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2564
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2565

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2566
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCD9-241224/2567
Product: wcn3610_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2568
Product: wcn3615_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2569
Product: wcn3620_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2570
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2571

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2572
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2573
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2574
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN	https://docs.qualcomm.com/pro	O-QUA-WCN3-241224/2575

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			target diagnostic information. **CVE ID : CVE-2024-43053**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2576
Product: wcn3660b_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2577
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	https://docs.qualcomm.com/product/pu	O-QUA-WCN3-241224/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-43048	blicresources/securitybulletin/december-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2579
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2580
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/de	O-QUA-WCN3-241224/2581

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2582
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2583
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2584

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2585
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2586
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2587
Product: wcn3680b_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2588
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2589
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2590
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as	https://docs.qualcomm.com/pro	O-QUA-WCN3-241224/2591

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2592
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2593
Product: wcn3680_firmware					
Affected Version(s): -					
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/pu	O-QUA-WCN3-241224/2594

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				blicresources/securitybulletin/december-2024-bulletin.html	
Product: wcn3950_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2595
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2596
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicreso	O-QUA-WCN3-241224/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	urces/securitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2598
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2599
Product: wcn3980_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-WCN3-241224/2600

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2601
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2602
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCN3-241224/2603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2604
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2605
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2606
Product: wcn3988_firmware					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2607
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2608
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2609
Use of Out-of-range	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in	https://docs.qua	O-QUA-WCN3-241224/2610

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pointer Offset			camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2611
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2612
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicreso	O-QUA-WCN3-241224/2613

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2614
Product: wcn3990_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2615
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/se	O-QUA-WCN3-241224/2616

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				curitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2617
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN3-241224/2618
Product: wcn3999_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WCN3-241224/2619

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wcn6740_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN6-241224/2620
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN6-241224/2621
Product: wcn6755_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicreso	O-QUA-WCN6-241224/2622

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				urces/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN6-241224/2623
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN6-241224/2624
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-	O-QUA-WCN6-241224/2625

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				2024-bulletin.html	
Product: wcn7860_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2626
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2627
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCN7-241224/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2629
Product: wcn7861_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2630
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCN7-241224/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2632
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2633
Product: wcn7880_firmware					
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WCN7-241224/2634

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2635
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2636
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2637
Product: wcn7881_firmware					

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

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2638
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2639
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WCN7-241224/2640
Integer Overflow	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a	https://docs.qua	O-QUA-WCN7-241224/2641

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
or Wraparound			beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	lcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	
Product: wsa8810_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2642
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2643
Stack-based	02-Dec-2024	7.8	Memory corruption when invalid input is passed to	https://docs.qualcomm.c	O-QUA-WSA8-241224/2644

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	om/product/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2645
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2646
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead	https://docs.qualcomm.com/product/publicresources/se	O-QUA-WSA8-241224/2647

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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 huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	curitybulletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2648
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2649
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2650

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Product: wsa8815_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2651
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2652
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2653

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2654
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2655
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2656

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2657
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2658
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2659
Product: wsa8830_firmware					
Affected Version(s): -					

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2660
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2661
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2662
Improper Restriction of Operations	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic	https://docs.qualcomm.com/pro	O-QUA-WSA8-241224/2663

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			private command inside WLAN driver. **CVE ID : CVE-2024-43049**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2664
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2665
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WSA8-241224/2666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2667
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2668
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2669

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2670
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2671
Product: wsa8832_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2672

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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	
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2673
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2674
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2675

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2676
Product: wsa8835_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2677
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2678

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2679
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2680
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2681
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input.	https://docs.qualcomm.com/pro	O-QUA-WSA8-241224/2682

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-43052	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2683
Use of Out-of-range Pointer Offset	02-Dec-2024	6.7	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access. **CVE ID : CVE-2024-33036**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2684
Untrusted Pointer Dereference	02-Dec-2024	6.7	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service. **CVE ID : CVE-2024-33039**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WSA8-241224/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Use After Free	02-Dec-2024	6.7	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access. **CVE ID : CVE-2024-33040**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2686
Use After Free	02-Dec-2024	6.7	Memory corruption when multiple threads try to unregister the CVP buffer at the same time. **CVE ID : CVE-2024-33053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2687
Buffer Over-read	02-Dec-2024	6.1	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware. **CVE ID : CVE-2024-33037**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2688

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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: wsa8840_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2689
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2690
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-	O-QUA-WSA8-241224/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2692
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2693
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2695
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2696
Product: wsa8845h_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2697

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2698
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2699
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2700
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory	https://docs.qualcomm.com/pro	O-QUA-WSA8-241224/2701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			test command inside WLAN driver. **CVE ID : CVE-2024-43050**	duct/publicresources/securitybulletin/december-2024-bulletin.html	
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2702
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2703
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybu	O-QUA-WSA8-241224/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				lletin/december-2024-bulletin.html	
Product: wsa8845_firmware					
Affected Version(s): -					
Improper Validation of Array Index	02-Dec-2024	8.4	Memory corruption while Configuring the SMR/S2CR register in Bypass mode. **CVE ID : CVE-2024-33044**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2705
Buffer Over-read	02-Dec-2024	8.4	Memory corruption when allocating and accessing an entry in an SMEM partition continuously. **CVE ID : CVE-2024-33056**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2706
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption when invalid input is passed to invoke GPU Headroom API call. **CVE ID : CVE-2024-43048**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2707

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				cember-2024-bulletin.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver. **CVE ID : CVE-2024-43049**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2708
Stack-based Buffer Overflow	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver. **CVE ID : CVE-2024-43050**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2709
Improper Input Validation	02-Dec-2024	7.8	Memory corruption while processing API calls to NPU with invalid input. **CVE ID : CVE-2024-43052**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2710

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Dec-2024	7.8	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information. **CVE ID : CVE-2024-43053**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2711
Integer Overflow or Wraparound	02-Dec-2024	7.5	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present. **CVE ID : CVE-2024-33063**	https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2024-bulletin.html	O-QUA-WSA8-241224/2712
Vendor: ruijienetworks					
Product: reyee_os					
Affected Version(s): From (including) 2.206.0 Up to (excluding) 2.320.0					
Server-Side Request Forgery (SSRF)	06-Dec-2024	9.8	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could give attackers the ability to force Ruijie's proxy servers to perform any request the attackers choose. Using this, attackers could access internal services used by Ruijie and their internal cloud infrastructure via AWS cloud metadata services.	N/A	O-RUI-REYE-241224/2713

CVSSv3 Scoring Scale	0-1	1-2	2-3	3-4	4-5	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-2024-48874		
Use of Inherently Dangerous Function	06-Dec-2024	9.8	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x uses an inherently dangerous function which could allow an attacker to send a malicious MQTT message resulting in devices executing arbitrary OS commands. **CVE ID : CVE-2024-52324**	N/A	O-RUI-REYE-241224/2714
Weak Password Recovery Mechanism for Forgotten Password	06-Dec-2024	9.4	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a weak mechanism for its users to change their passwords which leaves authentication vulnerable to brute force attacks. **CVE ID : CVE-2024-47547**	N/A	O-RUI-REYE-241224/2715
Improper Handling of Insufficient Permissions or Privileges	06-Dec-2024	8.1	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow MQTT clients connecting with device credentials to send messages to some topics. Attackers with device credentials could issue commands to other devices on behalf of Ruijie's cloud. **CVE ID : CVE-2024-46874**	N/A	O-RUI-REYE-241224/2716
Insecure Storage of Sensitive Information	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could enable an attacker to correlate a device serial number and the user's phone number and part of the email address.	N/A	O-RUI-REYE-241224/2717

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2024-47043		
N/A	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x uses weak credential mechanism that could allow an attacker to easily calculate MQTT credentials. **CVE ID : CVE-2024-45722**	N/A	O-RUI-REYE-241224/2718
Improper Neutralization of Wildcards or Matching Symbols	06-Dec-2024	7.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow an attacker to subscribe to partial possible topics in Ruijie MQTT broker, and receive partial messages being sent to and from devices. **CVE ID : CVE-2024-47791**	N/A	O-RUI-REYE-241224/2719
Exposure of Private Personal Information to an Unauthorized Actor	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a a feature that could enable sub accounts or attackers to view and exfiltrate sensitive information from all cloud accounts registered to Ruijie's services **CVE ID : CVE-2024-42494**	N/A	O-RUI-REYE-241224/2720
Premature Release of Resource During Expected Lifetime	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x contains a feature that could enable attackers to invalidate a legitimate user's session and cause a denial-of-service attack on a user's account. **CVE ID : CVE-2024-51727**	N/A	O-RUI-REYE-241224/2721

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

*stands for all versions

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Transmission of Private Resources into a New Sphere ('Resource Leak')	06-Dec-2024	6.5	Ruijie Reyee OS versions 2.206.x up to but not including 2.320.x could allow an attacker to obtain the devices serial number if physically adjacent and sniffing the RAW WIFI signal. **CVE ID : CVE-2024-47146**	N/A	O-RUI-REYE-241224/2722
Vendor: totolink					
Product: ex1800t_firmware					
Affected Version(s): 9.1.0cu.2112_b20220316					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-Dec-2024	4.3	A vulnerability classified as problematic was found in TOTOLINK EX1800T 9.1.0cu.2112_B20220316. This vulnerability affects the function sub_40662C of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12352**	N/A	O-TOT-EX18-241224/2723
Vendor: Tp-link					
Product: vn020_f3v_firmware					
Affected Version(s): 6.2.1021					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.5	A vulnerability classified as critical has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected is an unknown function of the file /control/WANIPConnection of the component SOAP Request Handler. The manipulation of the	https://www.tp-link.com/	O-TP--VN02-241224/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument NewConnectionType leads to buffer overflow. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12343**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Dec-2024	6.3	A vulnerability, which was classified as critical, was found in TP-Link VN020 F3v(T) TT_V6.2.1021. This affects an unknown part of the component FTP USER Command Handler. The manipulation leads to memory corruption. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. **CVE ID : CVE-2024-12344**	N/A	O-TP--VN02-241224/2725