https://nciipc.gov.in

National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures (CVE) Report

01 - 15 Feb 2025 Vol. 12 No. 03

## Table of Content

| Vendor | Product | Page Number |
|---|---|---|
| Qualcomm | robotics_rb5 | 293 |
| | sa6145p | 293 |
| | sa6150p | 294 |
| | sa6155 | 295 |
| | sa6155p | 295 |
| | sa7255p | 296 |
| | sa7775p | 297 |
| | sa8145p | 298 |
| | sa8150p | 299 |
| | sa8155 | 300 |
| | sa8155p | 300 |
| | sa8195p | 301 |
| | sa8255p | 303 |
| | sa8295p | 304 |
| | sa8530p | 305 |
| | sa8540p | 306 |
| | sa8620p | 308 |
| | sa8650p | 309 |
| | sa8770p | 310 |
| | sa8775p | 311 |
| | sa9000p | 312 |
| | sc8180x-aaab | 314 |
| | sc8180x-acaf | 314 |
| | sc8180x-ad | 315 |
| | sc8180xp-aaab | 315 |
| | sc8180xp-acaf | 316 |
| | sc8180xp-ad | 316 |
| | sc8280xp-abbb | 316 |
| | sc8380xp | 317 |
| | sd670 | 317 |
| | sd675 | 318 |
| | sd855 | 318 |
| | sd865_5g | 318 |

| Vendor | Product | Page Number |
|---|---|---|
| **Zyxel** | vmg4325-b10a_firmware | 796 |
| | vmg4380-b10a_firmware | 797 |
| | vmg8324-b10a_firmware | 797 |
| | vmg8924-b10a_firmware | 798 |

# Common Vulnerabilities and Exposures (CVE) Report

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Application** | | | | | |
| **Vendor: Adobe** | | | | | |
| **Product: experience_manager** | | | | | |
| Affected Version(s): * Up to (excluding) 2024.11.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low privileged 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. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.<br>**CVE ID: CVE-2024-53963** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/1 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low 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.<br>**CVE ID: CVE-2024-53964** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/2 |
| Improper Neutralization of Input During Web | 05-Feb-2025 | 5.4 | Adobe Experience Manager versions 6.5.21 and earlier are affected by a DOM-based Cross-Site Scripting | https://helpx.adobe.com/security/products/experience- | A-ADO-EXPE-170225/3 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Page Generation ('Cross-site Scripting') | | | (XSS) vulnerability that could be exploited by a low privileged 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. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.<br>**CVE ID: CVE-2024-53965** | manager/apsb24-69.html | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low 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.<br>**CVE ID: CVE-2024-53966** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/4 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low 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.<br>**CVE ID: CVE-2024-53962** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/5 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (excluding) 6.5.22 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low 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.<br>**CVE ID: CVE-2024-53962** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/6 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low privileged 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. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.<br>**CVE ID: CVE-2024-53963** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/7 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/8 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | browse to the page containing the vulnerable field.<br><br>**CVE ID: CVE-2024-53964** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low privileged 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. This type of attack requires user interaction, as the victim would need to access a manipulated link or input data into a vulnerable page.<br><br>**CVE ID: CVE-2024-53965** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/9 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 05-Feb-2025 | 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 a low 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.<br><br>**CVE ID: CVE-2024-53966** | https://helpx.adobe.com/security/products/experience-manager/apsb24-69.html | A-ADO-EXPE-170225/10 |
| **Vendor: angeljudesuarez** | | | | | |
| **Product: tailoring_management_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralizati | 01-Feb-2025 | 6.3 | A vulnerability classified as critical has been found in | N/A | A-ANG-TAIL-170225/11 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Special Elements in Output Used by a Downstream Component ('Injection') | | | itsourcecode Tailoring Management System 1.0. Affected is an unknown function of the file typedelete.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.<br><br>**CVE ID: CVE-2025-0945** | | |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 01-Feb-2025 | 6.3 | A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file deldoc.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.<br><br>**CVE ID: CVE-2025-0943** | N/A | A-ANG-TAIL-170225/12 |
| Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | 01-Feb-2025 | 6.3 | A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file customerview.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.<br><br>**CVE ID: CVE-2025-0944** | N/A | A-ANG-TAIL-170225/13 |
| Improper Neutralization of Special Elements in Output Used | 01-Feb-2025 | 6.3 | A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this | N/A | A-ANG-TAIL-170225/14 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| by a Downstream Component ('Injection') | | | vulnerability is an unknown functionality of the file templatedelete.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.<br>**CVE ID: CVE-2025-0946** | | |
| **Vendor: Apache** | | | | | |
| **Product: james_server** | | | | | |
| Affected Version(s): * Up to (excluding) 3.7.6 | | | | | |
| Uncontrolled Resource Consumption | 06-Feb-2025 | 6.5 | Apache James server JMAP HTML to text plain implementation in versions below 3.8.2 and 3.7.6 is subject to unbounded memory consumption that can result in a denial of service.<br><br>Users are recommended to upgrade to version 3.7.6 and 3.8.2, which fix this issue.<br>**CVE ID: CVE-2024-45626** | N/A | A-APA-JAME-170225/15 |
| Affected Version(s): From (including) 3.8.0 Up to (excluding) 3.8.2 | | | | | |
| Uncontrolled Resource Consumption | 06-Feb-2025 | 6.5 | Apache James server JMAP HTML to text plain implementation in versions below 3.8.2 and 3.7.6 is subject to unbounded memory consumption that can result in a denial of service.<br><br>Users are recommended to upgrade to version 3.7.6 and 3.8.2, which fix this issue.<br>**CVE ID: CVE-2024-45626** | N/A | A-APA-JAME-170225/16 |
| **Vendor: blackandwhitedigital** | | | | | |
| **Product: bookpress** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): * Up to (including) 1.2.7 | | | | | |
| Missing Authorization | 07-Feb-2025 | 8.2 | Missing Authorization vulnerability in blackandwhitedigital BookPress – For Book Authors allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects BookPress – For Book Authors: from n/a through 1.2.7.<br>**CVE ID: CVE-2025-25167** | N/A | A-BLA-BOOK-170225/17 |
| Cross-Site Request Forgery (CSRF) | 07-Feb-2025 | 7.1 | Cross-Site Request Forgery (CSRF) vulnerability in blackandwhitedigital BookPress – For Book Authors allows Cross-Site Scripting (XSS). This issue affects BookPress – For Book Authors: from n/a through 1.2.7.<br>**CVE ID: CVE-2025-25168** | N/A | A-BLA-BOOK-170225/18 |
| **Vendor: gabrieldarezzo** | | | | | |
| **Product: inlocation** | | | | | |
| Affected Version(s): * Up to (including) 1.8 | | | | | |
| Cross-Site Request Forgery (CSRF) | 07-Feb-2025 | 7.1 | Cross-Site Request Forgery (CSRF) vulnerability in gabrieldarezzo InLocation allows Stored XSS. This issue affects InLocation: from n/a through 1.8.<br>**CVE ID: CVE-2025-25166** | N/A | A-GAB-INLO-170225/19 |
| **Vendor: hasthemes** | | | | | |
| **Product: ht_mega** | | | | | |
| Affected Version(s): * Up to (excluding) 2.7.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-Feb-2025 | 6.4 | The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'block_css' and 'inner_css' parameters in all versions up to, and including, 2.7.6 | https://plugins.trac.wordpress.org/changeset/3209697/ht-mega-for-elementor | A-HAS-HT_M-170225/20 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.<br>**CVE ID: CVE-2024-12597** | | |
| **Vendor: IBM** | | | | | |
| **Product: applinx** | | | | | |
| Affected Version(s): 11.1.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-Feb-2025 | 6.4 | IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**CVE ID: CVE-2024-49791** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/21 |
| Use of a Broken or Risky Cryptographic Algorithm | 06-Feb-2025 | 5.9 | IBM ApplinX 11.1 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.<br>**CVE ID: CVE-2024-49797** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/22 |
| Improper Restriction of Rendered UI Layers or Frames | 06-Feb-2025 | 5.4 | IBM ApplinX 11.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/23 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | victim's click actions and possibly launch further attacks against the victim.<br>**CVE ID: CVE-2024-49796** | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-Feb-2025 | 5.4 | IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**CVE ID: CVE-2024-49792** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/24 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 06-Feb-2025 | 5.4 | IBM ApplinX 11.1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.<br>**CVE ID: CVE-2024-49793** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/25 |
| Cross-Site Request Forgery (CSRF) | 06-Feb-2025 | 4.3 | IBM ApplinX 11.1 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.<br>**CVE ID: CVE-2024-49794** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/26 |
| Cross-Site Request Forgery (CSRF) | 06-Feb-2025 | 4.3 | IBM ApplinX 11.1 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.<br>**CVE ID: CVE-2024-49795** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/27 |
| Generation of Error | 06-Feb-2025 | 4.3 | IBM ApplinX 11.1 could allow a remote attacker to | https://www.ibm.com/support/ | A-IBM-APPL-170225/28 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Message Containing Sensitive Information | | | obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.<br>**CVE ID: CVE-2024-49798** | pages/node/7182522 | |
| Cleartext Storage of Sensitive Information in Memory | 06-Feb-2025 | 4.3 | IBM ApplinX 11.1 stores sensitive information in cleartext in memory that could be obtained by an authenticated user.<br>**CVE ID: CVE-2024-49800** | https://www.ibm.com/support/pages/node/7182522 | A-IBM-APPL-170225/29 |
| **Vendor: Ietf** | | | | | |
| **Product: generic_routing_encapsulation** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 05-Feb-2025 | 6.5 | GRE and GRE6 Protocols (RFC2784) do not validate or verify the source of a network packet allowing an attacker to spoof and route arbitrary traffic via an exposed network interface that can lead to spoofing, access control bypass, and other unexpected network behaviors.<br>This can be considered similar to CVE-2020-10136.<br>**CVE ID: CVE-2024-7595** | N/A | A-IET-GENE-170225/30 |
| **Product: generic_routing_encapsulation6** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 05-Feb-2025 | 6.5 | GRE and GRE6 Protocols (RFC2784) do not validate or verify the source of a network packet allowing an attacker to spoof and route arbitrary traffic via an exposed network interface that can lead to spoofing, access control bypass, and | N/A | A-IET-GENE-170225/31 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | other unexpected network behaviors.<br><br>This can be considered similar to CVE-2020-10136.<br>**CVE ID: CVE-2024-7595** | | |
| **Product: generic_udp_encapsulation** | | | | | |
| Affected Version(s): - | | | | | |
| N/A | 05-Feb-2025 | 6.5 | Proposed Generic UDP Encapsulation (GUE) (IETF Draft) do not validate or verify the source of a network packet allowing an attacker to spoof and route arbitrary traffic via an exposed network interface that can lead to spoofing, access control bypass, and other unexpected network behaviors.<br><br>This can be considered similar to CVE-2020-10136.<br>**CVE ID: CVE-2024-7596** | N/A | A-IET-GENE-170225/32 |
| **Vendor: ivanti** | | | | | |
| **Product: connect_secure** | | | | | |
| Affected Version(s): * Up to (excluding) 22.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 11-Feb-2025 | 6.1 | Reflected XSS in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.<br>**CVE ID: CVE-2024-13830** | https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs | A-IVA-CONN-170225/33 |
| Affected Version(s): 22.7 | | | | | |
| Improper Neutralizati | 11-Feb-2025 | 6.1 | Reflected XSS in Ivanti Connect Secure before | https://forums.ivanti.com/s/arti | A-IVA-CONN-170225/34 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Input During Web Page Generation ('Cross-site Scripting') | | | version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.<br>**CVE ID: CVE-2024-13830** | cle/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs | |
| **Product: policy_secure** | | | | | |
| Affected Version(s): * Up to (excluding) 22.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 11-Feb-2025 | 6.1 | Reflected XSS in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.<br>**CVE ID: CVE-2024-13830** | https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs | A-IVA-POLI-170225/35 |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 11-Feb-2025 | 6.1 | Reflected XSS in Ivanti Connect Secure before version 22.7R2.6 and Ivanti Policy Secure before version 22.7R1.3 allows a remote unauthenticated attacker to obtain admin privileges. User interaction is required.<br>**CVE ID: CVE-2024-13830** | https://forums.ivanti.com/s/article/February-Security-Advisory-Ivanti-Connect-Secure-ICS-Ivanti-Policy-Secure-IPS-and-Ivanti-Secure-Access-Client-ISAC-Multiple-CVEs | A-IVA-POLI-170225/36 |
| **Vendor: Linuxfoundation** | | | | | |
| **Product: yocto** | | | | | |
| Affected Version(s): 4.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | A-LIN-YOCT-170225/37 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | | |
| **Vendor: markbarnes** | | | | | |
| **Product: style_tweaker** | | | | | |
| Affected Version(s): * Up to (including) 0.11 | | | | | |
| Cross-Site Request Forgery (CSRF) | 07-Feb-2025 | 7.1 | Cross-Site Request Forgery (CSRF) vulnerability in Mark Barnes Style Tweaker allows Stored XSS. This issue affects Style Tweaker: from n/a through 0.11.<br>**CVE ID: CVE-2025-25160** | N/A | A-MAR-STYL-170225/38 |
| **Vendor: mediatek** | | | | | |
| **Product: software_development_kit** | | | | | |
| Affected Version(s): * Up to (including) 7.4.0.1 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 8.8 | In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00400889; Issue ID: MSV-2491.<br>**CVE ID: CVE-2025-20633** | https://corp.mediatek.com/product-security-bulletin/February-2025 | A-MED-SOFT-170225/39 |
| Affected Version(s): * Up to (including) 7.6.7.0 | | | | | |
| Uncaught Exception | 03-Feb-2025 | 7.5 | In network HW, there is a possible system hang due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00399035; Issue ID: MSV-2380. | https://corp.mediatek.com/product-security-bulletin/February-2025 | A-MED-SOFT-170225/40 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20637** | | |
| **Vendor: Microsoft** | | | | | |
| **Product: 365_apps** | | | | | |
| Affected Version(s): - | | | | | |
| Use After Free | 11-Feb-2025 | 7.8 | Microsoft Office Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21397** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21397 | A-MIC-365_-170225/41 |
| **Product: autoupdate** | | | | | |
| Affected Version(s): * Up to (excluding) 4.77.24121924 | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 11-Feb-2025 | 7 | Microsoft AutoUpdate (MAU) Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-24036** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24036 | A-MIC-AUTO-170225/42 |
| **Product: dynamics_365_sales** | | | | | |
| Affected Version(s): - | | | | | |
| Server-Side Request Forgery (SSRF) | 06-Feb-2025 | 8.7 | Server-Side Request Forgery (SSRF) in Microsoft Dynamics 365 Sales allows an authorized attacker to elevate privileges over a network.<br>**CVE ID: CVE-2025-21177** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21177 | A-MIC-DYNA-170225/43 |
| **Product: edge** | | | | | |
| Affected Version(s): - | | | | | |
| User Interface (UI) Misrepresentation of Critical Information | 06-Feb-2025 | 5.3 | Microsoft Edge for IOS and Android Spoofing Vulnerability<br>**CVE ID: CVE-2025-21253** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21253 | A-MIC-EDGE-170225/44 |
| **Product: edge_chromium** | | | | | |
| Affected Version(s): * Up to (excluding) 133.0.3065.51 | | | | | |
| Access of Resource Using Incompatible Type | 06-Feb-2025 | 8.8 | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | A-MIC-EDGE-170225/45 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Type Confusion') | | | **CVE ID: CVE-2025-21342** | 21342 | |
| Access of Resource Using Incompatible Type ('Type Confusion') | 06-Feb-2025 | 8.8 | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21408** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21408 | A-MIC-EDGE-170225/46 |
| Access of Resource Using Incompatible Type ('Type Confusion') | 06-Feb-2025 | 6.5 | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21279** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21279 | A-MIC-EDGE-170225/47 |
| Insufficient Granularity of Address Regions Protected by Register Locks | 06-Feb-2025 | 6.5 | Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21283** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21283 | A-MIC-EDGE-170225/48 |
| Improperly Implemented Security Check for Standard | 06-Feb-2025 | 4.4 | Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID: CVE-2025-21267** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21267 | A-MIC-EDGE-170225/49 |
| The UI Performs the Wrong Action | 06-Feb-2025 | 4.3 | Microsoft Edge (Chromium-based) Spoofing Vulnerability **CVE ID: CVE-2025-21404** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21404 | A-MIC-EDGE-170225/50 |
| **Product: office** | | | | | |
| Affected Version(s): 2021 | | | | | |
| Use After Free | 11-Feb-2025 | 7.8 | Microsoft Office Remote Code Execution Vulnerability **CVE ID: CVE-2025-21397** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21397 | A-MIC-OFFI-170225/51 |
| Affected Version(s): 2024 | | | | | |
| Use After Free | 11-Feb-2025 | 7.8 | Microsoft Office Remote Code Execution Vulnerability **CVE ID: CVE-2025-21397** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | A-MIC-OFFI-170225/52 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 21397 | |
| **Product: sharepoint_server** | | | | | |
| Affected Version(s): * Up to (excluding) 16.0.17928.20396 | | | | | |
| Improper Authorization | 11-Feb-2025 | 8 | Microsoft SharePoint Server Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21400** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21400 | A-MIC-SHAR-170225/53 |
| Affected Version(s): 2016 | | | | | |
| Improper Authorization | 11-Feb-2025 | 8 | Microsoft SharePoint Server Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21400** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21400 | A-MIC-SHAR-170225/54 |
| Affected Version(s): 2019 | | | | | |
| Improper Authorization | 11-Feb-2025 | 8 | Microsoft SharePoint Server Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21400** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21400 | A-MIC-SHAR-170225/55 |
| **Vendor: Mozilla** | | | | | |
| **Product: firefox** | | | | | |
| Affected Version(s): * Up to (excluding) 115.20.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1016** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/56 |
| Use After Free | 04-Feb-2025 | 9.8 | An attacker could have caused a use-after-free via | https://www.mozilla.org/securi | A-MOZ-FIRE-170225/57 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted XSLT data, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1009** | ty/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Use After Free | 04-Feb-2025 | 8.8 | An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1010** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/58 |
| Use After Free | 04-Feb-2025 | 7.5 | A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1012** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/59 |
| Affected Version(s): * Up to (excluding) 128.7.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. Some of | https://www.mozilla.org/security/advisories/mfsa2025-07/, | A-MOZ-FIRE-170225/60 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1017** | https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | |
| N/A | 04-Feb-2025 | 8.8 | A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1011** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/61 |
| Improper Certificate Validation | 04-Feb-2025 | 8.8 | Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1014** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/62 |
| Affected Version(s): * Up to (excluding) 135.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/securi | A-MOZ-FIRE-170225/63 |

| 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 |
|---|---|---|---|---|---|
| | | | these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1016** | ty/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134 and Thunderbird 134. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135 and Thunderbird < 135.<br>**CVE ID: CVE-2025-1020** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/64 |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1017** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/65 |
| Use After Free | 04-Feb-2025 | 9.8 | An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, | A-MOZ-FIRE-170225/66 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1009** | https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Use After Free | 04-Feb-2025 | 8.8 | An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1010** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/67 |
| Improper Certificate Validation | 04-Feb-2025 | 8.8 | Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1014** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/68 |
| N/A | 04-Feb-2025 | 8.8 | A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135. | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, | A-MOZ-FIRE-170225/69 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-1011** | https://www.mozilla.org/security/advisories/mfsa2025-11/ | |
| Use After Free | 04-Feb-2025 | 7.5 | A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1012** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/70 |
| Improper Restriction of Rendered UI Layers or Frames | 04-Feb-2025 | 5.3 | The fullscreen notification is prematurely hidden when fullscreen is re-requested quickly by the user. This could have been leveraged to perform a potential spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.<br>**CVE ID: CVE-2025-1018** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/71 |
| Improper Restriction of Rendered UI Layers or Frames | 04-Feb-2025 | 4.3 | The z-order of the browser windows could be manipulated to hide the fullscreen notification. This could potentially be leveraged to perform a spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.<br>**CVE ID: CVE-2025-1019** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-FIRE-170225/72 |
| Affected Version(s): From (including) 128.1.0 Up to (excluding) 128.7.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/securi | A-MOZ-FIRE-170225/73 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1016** | ty/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Use After Free | 04-Feb-2025 | 9.8 | An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1009** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/74 |
| Use After Free | 04-Feb-2025 | 8.8 | An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1010** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-FIRE-170225/75 |
| Use After Free | 04-Feb-2025 | 7.5 | A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/securi | A-MOZ-FIRE-170225/76 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1012** | ty/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| **Product: thunderbird** | | | | | |
| Affected Version(s): * Up to (excluding) 135.0 | | | | | |
| N/A | 04-Feb-2025 | 8.8 | A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1011** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/77 |
| Use After Free | 04-Feb-2025 | 7.5 | A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1012** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/78 |
| Affected Version(s): From (including) 128.0.1 Up to (excluding) 128.7.0 | | | | | |
| Use After Free | 04-Feb-2025 | 9.8 | An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash. This vulnerability | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.m | A-MOZ-THUN-170225/79 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1009** | ozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1016** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/80 |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1017** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/81 |
| Improper Certificate Validation | 04-Feb-2025 | 8.8 | Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed. This | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.m | A-MOZ-THUN-170225/82 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1014** | ozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | |
| N/A | 04-Feb-2025 | 8.8 | A bug in WebAssembly code generation could have lead to a crash. It may have been possible for an attacker to leverage this to achieve code execution. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1011** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/83 |
| Use After Free | 04-Feb-2025 | 8.8 | An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1010** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/84 |
| Use After Free | 04-Feb-2025 | 7.5 | A race during concurrent delazification could have led to a use-after-free. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135. | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.m | A-MOZ-THUN-170225/85 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-1012** | ozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| N/A | 04-Feb-2025 | 6.5 | Thunderbird displayed an incorrect sender address if the From field of an email used the invalid group name syntax that is described in CVE-2024-49040. This vulnerability affects Thunderbird < 128.7 and Thunderbird < 135.<br>**CVE ID: CVE-2025-0510** | https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/86 |
| N/A | 04-Feb-2025 | 5.4 | The Thunderbird Address Book URI fields contained unsanitized links. This could be used by an attacker to create and export an address book containing a malicious payload in a field. For example, in the "Other" field of the Instant Messaging section. If another user imported the address book, clicking on the link could result in opening a web page inside Thunderbird, and that page could execute (unprivileged) JavaScript. This vulnerability affects Thunderbird < 128.7.<br>**CVE ID: CVE-2025-1015** | https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/87 |
| Affected Version(s): From (including) 131.0 Up to (excluding) 135.0 | | | | | |
| Use After Free | 04-Feb-2025 | 9.8 | An attacker could have caused a use-after-free via crafted XSLT data, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135. | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/m | A-MOZ-THUN-170225/88 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-1009** | fsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 115.19, Firefox ESR 128.6, Thunderbird 115.19, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1016** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/89 |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134, Thunderbird 134, Firefox ESR 128.6, and Thunderbird 128.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1017** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/90 |
| Out-of-bounds Write | 04-Feb-2025 | 9.8 | Memory safety bugs present in Firefox 134 and Thunderbird 134. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 135 and Thunderbird < | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/91 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 135.<br>**CVE ID: CVE-2025-1020** | | |
| Improper Certificate Validation | 04-Feb-2025 | 8.8 | Certificate length was not properly checked when added to a certificate store. In practice only trusted data was processed. This vulnerability affects Firefox < 135, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1014** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/92 |
| Use After Free | 04-Feb-2025 | 8.8 | An attacker could have caused a use-after-free via the Custom Highlight API, leading to a potentially exploitable crash. This vulnerability affects Firefox < 135, Firefox ESR < 115.20, Firefox ESR < 128.7, Thunderbird < 128.7, and Thunderbird < 135.<br>**CVE ID: CVE-2025-1010** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-08/, https://www.mozilla.org/security/advisories/mfsa2025-09/, https://www.mozilla.org/security/advisories/mfsa2025-10/ | A-MOZ-THUN-170225/93 |
| N/A | 04-Feb-2025 | 6.5 | Thunderbird displayed an incorrect sender address if the From field of an email used the invalid group name syntax that is described in CVE-2024-49040. This vulnerability affects Thunderbird < 128.7 and Thunderbird < 135.<br>**CVE ID: CVE-2025-0510** | https://www.mozilla.org/security/advisories/mfsa2025-10/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/94 |
| Improper Restriction of Rendered UI Layers or Frames | 04-Feb-2025 | 5.3 | The fullscreen notification is prematurely hidden when fullscreen is re-requested quickly by the user. This could have been leveraged | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.m | A-MOZ-THUN-170225/95 |

| 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 |
|---|---|---|---|---|---|
| | | | to perform a potential spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.<br><br>**CVE ID: CVE-2025-1018** | ozilla.org/security/advisories/mfsa2025-11/ | |
| Improper Restriction of Rendered UI Layers or Frames | 04-Feb-2025 | 4.3 | The z-order of the browser windows could be manipulated to hide the fullscreen notification. This could potentially be leveraged to perform a spoofing attack. This vulnerability affects Firefox < 135 and Thunderbird < 135.<br><br>**CVE ID: CVE-2025-1019** | https://www.mozilla.org/security/advisories/mfsa2025-07/, https://www.mozilla.org/security/advisories/mfsa2025-11/ | A-MOZ-THUN-170225/96 |
| **Vendor: pdf-xchange** | | | | | |
| **Product: pdf-xchange_editor** | | | | | |
| Affected Version(s): * Up to (excluding) 10.4.1.389 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | PDF-XChange Editor AcroForm Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the handling of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25349. | N/A | A-PDF-PDF--170225/97 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-0899** | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor Doc Object Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the handling of Doc objects. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25372.<br><br>**CVE ID: CVE-2025-0901** | N/A | A-PDF-PDF--170225/98 |
| Affected Version(s): * Up to (excluding) 10.4.2.390 | | | | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of XPS files. The issue results from | N/A | A-PDF-PDF--170225/99 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25405.<br><br>**CVE ID: CVE-2025-0902** | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | PDF-XChange Editor RTF File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of RTF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-25421.<br><br>**CVE ID: CVE-2025-0903** | N/A | A-PDF-PDF--170225/100 |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on | N/A | A-PDF-PDF--170225/101 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of XPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25422.<br><br>**CVE ID: CVE-2025-0904** | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of JB2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current | N/A | A-PDF-PDF--170225/102 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | process. Was ZDI-CAN-25433.<br><br>**CVE ID: CVE-2025-0905** | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of JB2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25434.<br><br>**CVE ID: CVE-2025-0906** | N/A | A-PDF-PDF--170225/103 |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor JB2 File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists | N/A | A-PDF-PDF--170225/104 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | within the parsing of JB2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25435.<br><br>**CVE ID: CVE-2025-0907** | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25557.<br><br>**CVE ID: CVE-2025-0908** | N/A | A-PDF-PDF--170225/105 |
| Affected Version(s): * Up to (excluding) 10.5.0.393 | | | | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor XPS File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. | N/A | A-PDF-PDF--170225/106 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of XPS files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25678.<br><br>**CVE ID: CVE-2025-0909** | | |
| Out-of-bounds Write | 11-Feb-2025 | 8.8 | PDF-XChange Editor U3D File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability | N/A | A-PDF-PDF--170225/107 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to execute code in the context of the current process. Was ZDI-CAN-25748.<br><br>**CVE ID: CVE-2025-0910** | | |
| Out-of-bounds Read | 11-Feb-2025 | 8.8 | PDF-XChange Editor U3D File Parsing Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of PDF-XChange Editor. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.<br><br>The specific flaw exists within the parsing of U3D files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-25957.<br><br>**CVE ID: CVE-2025-0911** | N/A | A-PDF-PDF--170225/108 |
| **Vendor: phpgurukul** | | | | | |
| **Product: daily_expense_tracker_system** | | | | | |
| Affected Version(s): 1.1 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 12-Feb-2025 | 9.8 | PHPGurukul Daily Expense Tracker System v1.1 is vulnerable to SQL Injection in /dets/add-expense.php via the costitem parameter.<br><br>**CVE ID: CVE-2025-25349** | N/A | A-PHP-DAIL-170225/109 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 12-Feb-2025 | 9.8 | PHPGurukul Daily Expense Tracker System v1.1 is vulnerable to SQL Injection in /dets/add-expense.php via the dateexpense parameter.<br>**CVE ID: CVE-2025-25351** | N/A | A-PHP-DAIL-170225/110 |
| **Product: land_record_system** | | | | | |
| Affected Version(s): 1.0 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 13-Feb-2025 | 7.2 | A SQL Injection vulnerability was found in /admin/aboutus.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the pagetitle POST request parameter.<br>**CVE ID: CVE-2025-25352** | N/A | A-PHP-LAND-170225/111 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 13-Feb-2025 | 7.2 | A SQL Injection was found in /admin/admin-profile.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the contactnumber POST request parameter.<br>**CVE ID: CVE-2025-25354** | N/A | A-PHP-LAND-170225/112 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 13-Feb-2025 | 7.2 | A SQL Injection vulnerability was found in /admin/bwdates-reports-details.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the fromdate POST request parameter.<br>**CVE ID: CVE-2025-25355** | N/A | A-PHP-LAND-170225/113 |
| Improper Neutralization of Special Elements used in an | 13-Feb-2025 | 7.2 | A SQL Injection vulnerability was found in /admin/bwdates-reports-details.php in PHPGurukul Land Record System v1.0, | N/A | A-PHP-LAND-170225/114 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| SQL Command ('SQL Injection') | | | which allows remote attackers to execute arbitrary code via the " todate" POST request parameter.<br>**CVE ID: CVE-2025-25356** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 13-Feb-2025 | 7.2 | A SQL Injection vulnerability was found in /admin/contactus.php in PHPGurukul Land Record System v1.0, which allows remote attackers to execute arbitrary code via the email POST request parameter.<br>**CVE ID: CVE-2025-25357** | N/A | A-PHP-LAND-170225/115 |
| **Vendor: pluginab** | | | | | |
| **Product: plugin_a\/b_image_optimizer** | | | | | |
| Affected Version(s): * Up to (including) 3.3 | | | | | |
| Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | 07-Feb-2025 | 7.5 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Zach Swetz Plugin A/B Image Optimizer allows Path Traversal. This issue affects Plugin A/B Image Optimizer: from n/a through 3.3.<br>**CVE ID: CVE-2025-25163** | N/A | A-PLU-PLUG-170225/116 |
| **Vendor: posimyth** | | | | | |
| **Product: the_plus_addons_for_elementor** | | | | | |
| Affected Version(s): * Up to (excluding) 6.2.0 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 01-Feb-2025 | 6.4 | The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Table Widget's searchable_label parameter in all versions up to, and including, 6.1.8 due to insufficient input sanitization and output escaping. This makes it | https://plugins.trac.wordpress.org/changeset/3207945/the-plus-addons-for-elementor-page-builder/tags/6.1.2/modules/widgets/tp_table.php?old=3207456&old_path=the-plus-addons-for-elementor-page-builder%2Ftags | A-POS-THE_-170225/117 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.<br>**CVE ID: CVE-2024-11829** | %2F6.1.1%2Fmodules%2Fwidgets%2Ftp_table.php | |
| **Vendor: qodeinteractive** | | | | | |
| **Product: qi_addons_for_elementor** | | | | | |
| Affected Version(s): * Up to (including) 1.8.7 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-Feb-2025 | 6.4 | The Qi Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cursor' parameter in all versions up to, and including, 1.8.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in versions 1.8.5, 1.8.6, and 1.8.7.<br>**CVE ID: CVE-2024-13699** | https://plugins.trac.wordpress.org/changeset/3230342/, https://plugins.trac.wordpress.org/changeset/3231980/, https://plugins.trac.wordpress.org/changeset/3232550/, https://plugins.trac.wordpress.org/changeset/3234136/ | A-QOD-QI_A-170225/118 |
| **Vendor: rdkcentral** | | | | | |
| **Product: rdk-b** | | | | | |
| Affected Version(s): 2022q3 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | A-RDK-RDK--170225/119 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | | |
| Affected Version(s): 2024q1 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | A-RDK-RDK--170225/120 |
| **Vendor: scriptsbundle** | | | | | |
| **Product: dwt_listing** | | | | | |
| Affected Version(s): * Up to (excluding) 3.3.5 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 08-Feb-2025 | 6.4 | The DWT - Directory & Listing WordPress Theme is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.3.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.<br>**CVE ID: CVE-2025-0169** | N/A | A-SCR-DWT_-170225/121 |
| **Vendor: soflyy** | | | | | |
| **Product: wp_all_export** | | | | | |
| Affected Version(s): * Up to (excluding) 1.9.2 | | | | | |
| Improper Control of | 07-Feb-2025 | 8.3 | The WP ALL Export Pro plugin for WordPress is | N/A | A-SOF-WP_A-170225/122 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Generation of Code ('Code Injection') | | | vulnerable to Remote Code Execution in all versions up to, and including, 1.9.1 via the custom export fields. This is due to the missing input validation and sanitization of user-supplied data. This makes it possible for unauthenticated attackers to inject arbitrary PHP code into form fields that get executed on the server during the export, potentially leading to a complete site compromise.<br><br>As a prerequisite, the custom export field should include fields containing user-supplied data.<br><br>**CVE ID: CVE-2024-7419** | | |
| Improper Control of Generation of Code ('Code Injection') | 07-Feb-2025 | 6.8 | The WP ALL Export Pro plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to improper user input validation and sanitization in all versions up to, and including, 1.9.1. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.<br><br>**CVE ID: CVE-2024-7425** | N/A | A-SOF-WP_A-170225/123 |
| **Product: wp_all_import** | | | | | |
| Affected Version(s): * Up to (excluding) 4.9.8 | | | | | |
| Deserializati | 07-Feb-2025 | 7.2 | The WP All Import Pro | N/A | A-SOF-WP_A- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Untrusted Data | | | plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.9.7 via deserialization of untrusted input from an import file. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.<br>**CVE ID: CVE-2024-9664** | | 170225/124 |
| **Vendor: superstorefinder** | | | | | |
| **Product: super_store_finder** | | | | | |
| Affected Version(s): * Up to (excluding) 7.1 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 09-Feb-2025 | 8.2 | The Super Store Finder plugin for WordPress is vulnerable to SQL Injection via the 'ssf_wp_user_name' parameter in all versions up to, and including, 7.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into an already existing query to store cross-site scripting in store reviews.<br>**CVE ID: CVE-2024-13440** | https://superstorefinder.net/support/forums/topic/super-store-finder-for-wordpress-patch-notes/ | A-SUP-SUPE-170225/125 |
| **Vendor: Trimble** | | | | | |
| **Product: cityworks** | | | | | |
| Affected Version(s): * Up to (excluding) 15.8.9 | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Deserialization of Untrusted Data | 06-Feb-2025 | 8.8 | Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10 are vulnerable to a deserialization vulnerability. This could allow an authenticated user to perform a remote code execution attack against a customer's Microsoft Internet Information Services (IIS) web server.<br>**CVE ID: CVE-2025-0994** | https://learn.assetlifecycle.trimble.com/i/1532182-cityworks-customer-communication-2025-02-05-docx/0? | A-TRI-CITY-170225/126 |
| Affected Version(s): From (including) 23.0 Up to (excluding) 23.10 | | | | | |
| Deserialization of Untrusted Data | 06-Feb-2025 | 8.8 | Trimble Cityworks versions prior to 15.8.9 and Cityworks with office companion versions prior to 23.10 are vulnerable to a deserialization vulnerability. This could allow an authenticated user to perform a remote code execution attack against a customer's Microsoft Internet Information Services (IIS) web server.<br>**CVE ID: CVE-2025-0994** | https://learn.assetlifecycle.trimble.com/i/1532182-cityworks-customer-communication-2025-02-05-docx/0? | A-TRI-CITY-170225/127 |
| **Vendor: wegia** | | | | | |
| **Product: wegia** | | | | | |
| Affected Version(s): * Up to (excluding) 3.2.12 | | | | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-Feb-2025 | 9.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_detalhes_socio.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version | https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-x28g-6228-99p9 | A-WEG-WEGI-170225/128 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24957** | | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-Feb-2025 | 9.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_detalhes_cobranca.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24906** | https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-jpph-g9p7-9jrm | A-WEG-WEGI-170225/129 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-Feb-2025 | 9.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `get_codigobarras_cobranca.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24905** | https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-qjc6-5qv6-fr8m | A-WEG-WEGI-170225/130 |
| Improper Neutralization of Special | 03-Feb-2025 | 8.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection | https://github.com/LabRedesCefetRJ/WeGIA/se | A-WEG-WEGI-170225/131 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Elements used in an SQL Command ('SQL Injection') | | | vulnerability was discovered in the WeGIA application, `salvar_tag.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24958** | curity/advisories/GHSA-2mhx-5998-46hx | |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-Feb-2025 | 8.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `salvar_cargo.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24902** | https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-pg73-w9vx-8mgp | A-WEG-WEGI-170225/132 |
| Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | 03-Feb-2025 | 8.8 | WeGIA is a Web Manager for Charitable Institutions. A SQL Injection vulnerability was discovered in the WeGIA application, `deletar_permissao.php` endpoint. This vulnerability could allow an authorized attacker to execute arbitrary SQL queries, allowing access to or deletion of sensitive | https://github.com/LabRedesCefetRJ/WeGIA/security/advisories/GHSA-jp48-94wm-3gmc | A-WEG-WEGI-170225/133 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information. This issue has been addressed in version 3.2.12 and all users are advised to upgrade. There are no known workarounds for this vulnerability.<br>**CVE ID: CVE-2025-24901** | | |
| **Vendor: wpjobportal** | | | | | |
| **Product: wp_job_portal** | | | | | |
| Affected Version(s): * Up to (excluding) 2.2.7 | | | | | |
| Missing Authorization | 01-Feb-2025 | 5.3 | The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to unauthorized arbitrary emails sending due to a missing capability check on the sendEmailToJobSeeker() function in all versions up to, and including, 2.2.6. This makes it possible for unauthenticated attackers to send arbitrary emails with arbitrary content from the sites mail server.<br>**CVE ID: CVE-2024-13371** | https://plugins.trac.wordpress.org/changeset/3229608/wp-job-portal/tags/2.2.7/modules/jobapply/model.php?old=3216415&old_path=wp-job-portal%2Ftags%2F2.2.6%2Fmodules%2Fjobapply%2Fmodel.php | A-WPJ-WP_J-170225/134 |
| Authorization Bypass Through User-Controlled Key | 01-Feb-2025 | 5.3 | The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2.6 via the getresumefiledownloadbyid() and getallresumefiles() functions due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to download users resumes without the appropriate authorization to do so. | https://plugins.trac.wordpress.org/changeset/3229608/wp-job-portal/tags/2.2.7/modules/resume/controller.php?old=3216415&old_path=wp-job-portal%2Ftags%2F2.2.6%2Fmodules%2Fresume%2Fcontroller.php | A-WPJ-WP_J-170225/135 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-13372** | | |
| Authorization Bypass Through User-Controlled Key | 01-Feb-2025 | 5.3 | The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2.6 via the deleteCompanyLogo() due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to delete arbitrary company logos.<br>**CVE ID: CVE-2024-13428** | https://plugins.trac.wordpress.org/changeset/3229608/wp-job-portal/tags/2.2.7/modules/company/model.php?old=3216415&old_path=wp-job-portal%2Ftags%2F2.2.6%2Fmodules%2Fcompany%2Fmodel.php | A-WPJ-WP_J-170225/136 |
| Authorization Bypass Through User-Controlled Key | 01-Feb-2025 | 4.3 | The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2.6 via the enforcedelete() function due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with Employer-level access and above, to delete other users companies.<br>**CVE ID: CVE-2024-13425** | https://plugins.trac.wordpress.org/changeset/3229608/wp-job-portal/tags/2.2.7/modules/company/controller.php?old=3216415&old_path=wp-job-portal%2Ftags%2F2.2.6%2Fmodules%2Fcompany%2Fcontroller.php | A-WPJ-WP_J-170225/137 |
| Authorization Bypass Through User-Controlled Key | 01-Feb-2025 | 4.3 | The WP Job Portal – A Complete Recruitment System for Company or Job Board website plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2.6 via the 'jobenforcedelete' due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with employer-level access | https://plugins.trac.wordpress.org/changeset/3229608/wp-job-portal/tags/2.2.7/modules/job/controller.php?old=3216415&old_path=wp-job-portal%2Ftags%2F2.2.6%2Fmodules%2Fjob%2Fcontroller.php | A-WPJ-WP_J-170225/138 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | and above, to delete arbitrary<br>**CVE ID: CVE-2024-13429** | | |
| **Vendor: wpmailster** | | | | | |
| **Product: wp_mailster** | | | | | |
| Affected Version(s): * Up to (excluding) 1.8.16 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 03-Feb-2025 | 7.1 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This issue affects WP Mailster: from n/a through 1.8.15.0.<br>**CVE ID: CVE-2025-24559** | N/A | A-WPM-WP_M-170225/139 |
| Affected Version(s): * Up to (excluding) 1.8.18 | | | | | |
| Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | 04-Feb-2025 | 7.1 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in brandtoss WP Mailster allows Reflected XSS. This issue affects WP Mailster: from n/a through 1.8.17.0.<br>**CVE ID: CVE-2025-24598** | N/A | A-WPM-WP_M-170225/140 |
| **Hardware** | | | | | |
| **Vendor: mediatek** | | | | | |
| **Product: mt2737** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT27-170225/141 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20634** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT27-170225/142 |
| **Product: mt6580** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT65-170225/143 |
| **Product: mt6739** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/144 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/145 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/146 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/147 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/148 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/149 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/150 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/151 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/152 |
| **Product: mt6761** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/153 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/154 |
| Write-what- | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible | https://corp.me | H-MED-MT67- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| where Condition | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | diatek.com/product-security-bulletin/February-2025 | 170225/155 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/156 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/157 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/158 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/159 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/160 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/161 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20643** | | |
| **Product: mt6765** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/162 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/163 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/164 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | H-MED-MT67-170225/165 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/166 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/167 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/168 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/169 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/170 |
| **Product: mt6768** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/171 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/172 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/173 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/174 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT67-170225/175 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/176 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/177 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/178 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/179 |
| **Product: mt6771** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/180 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/181 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/182 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/183 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/184 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT67-170225/185 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | bulletin/February-2025 | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/186 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/187 |
| **Product: mt6779** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/188 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/189 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/190 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/191 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20639** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/192 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/193 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/194 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT67-170225/195 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | ry-2025 | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/196 |
| **Product: mt6781** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/197 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/198 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/199 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/200 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/201 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20635** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/202 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/203 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/204 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT67-170225/205 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | ry-2025 | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/206 |
| **Product: mt6785** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/207 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/208 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/209 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/210 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/211 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20641** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/212 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/213 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/214 |
| Debug Messages Revealing Unnecessary | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT67-170225/215 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information | | | information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | ry-2025 | |
| **Product: mt6789** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/216 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT67-170225/217 |
| **Product: mt6813** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/218 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| **Product: mt6833** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/219 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/220 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/221 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/222 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/223 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/224 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20641** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/225 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/226 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/227 |
| **Product: mt6835** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 9.8 | In Modem, there is a | https://corp.me | H-MED-MT68- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | diatek.com/product-security-bulletin/February-2025 | 170225/228 |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/229 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/230 |
| **Product: mt6835t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT68-170225/231 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | ry-2025 | |
| **Product: mt6853** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/232 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/233 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/234 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/235 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/236 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/237 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20642** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/238 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/239 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/240 |
| **Product: mt6855** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 6.7 | In secmem, there is a | https://corp.me | H-MED-MT68- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | diatek.com/product-security-bulletin/February-2025 | 170225/241 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/242 |
| **Product: mt6873** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/243 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/244 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/245 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/246 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/247 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/248 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/249 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/250 |
| Debug Messages Revealing | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT68-170225/251 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unnecessary Information | | | could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | bulletin/February-2025 | |
| **Product: mt6877** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/252 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/253 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/254 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/255 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/256 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/257 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20642** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/258 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/259 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/260 |
| **Product: mt6878** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 9.8 | In Modem, there is a | https://corp.me | H-MED-MT68- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | diatek.com/product-security-bulletin/February-2025 | 170225/261 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/262 |
| **Product: mt6878m** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/263 |
| **Product: mt6879** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/264 |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/265 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/266 |
| **Product: mt6880** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible | https://corp.me | H-MED-MT68- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | diatek.com/product-security-bulletin/February-2025 | 170225/267 |
| **Product: mt6883** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/268 |
| **Product: mt6885** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/269 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT68-170225/270 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/271 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/272 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/273 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/274 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/275 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/276 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/277 |
| **Product: mt6886** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/278 |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/279 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT68-170225/280 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | bulletin/February-2025 | |
| **Product: mt6889** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/281 |
| **Product: mt6890** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/282 |
| **Product: mt6893** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 6.7 | In secmem, there is a | https://corp.me | H-MED-MT68- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | diatek.com/product-security-bulletin/February-2025 | 170225/283 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/284 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/285 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/286 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/287 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/288 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/289 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20640** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/290 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/291 |
| **Product: mt6895** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/292 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/293 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/294 |
| **Product: mt6895tt** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/295 |
| **Product: mt6896** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/296 |
| **Product: mt6897** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/297 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/298 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: mt6899** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT68-170225/299 |
| **Product: mt6980** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/300 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/301 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20635** | | |
| **Product: mt6980d** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/302 |
| **Product: mt6983** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/303 |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/304 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/305 |
| **Product: mt6983t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/306 |
| **Product: mt6985** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/307 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/308 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/309 |
| **Product: mt6985t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/310 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20634** | | |
| **Product: mt6989** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/311 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/312 |
| **Product: mt6989t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/313 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| **Product: mt6990** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/314 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/315 |
| **Product: mt6991** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT69-170225/316 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| **Product: mt7603** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 8.8 | In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00400889; Issue ID: MSV-2491.<br>**CVE ID: CVE-2025-20633** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT76-170225/317 |
| **Product: mt7615** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 8.8 | In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00400889; Issue ID: MSV-2491.<br>**CVE ID: CVE-2025-20633** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT76-170225/318 |
| **Product: mt7622** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 8.8 | In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT76-170225/319 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00400889; Issue ID: MSV-2491.<br>**CVE ID: CVE-2025-20633** | | |
| **Product: mt7915** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 8.8 | In wlan AP driver, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00400889; Issue ID: MSV-2491.<br>**CVE ID: CVE-2025-20633** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT79-170225/320 |
| **Product: mt7981** | | | | | |
| Affected Version(s): - | | | | | |
| Uncaught Exception | 03-Feb-2025 | 7.5 | In network HW, there is a possible system hang due to an uncaught exception. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00399035; Issue ID: MSV-2380.<br>**CVE ID: CVE-2025-20637** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT79-170225/321 |
| **Product: mt7986** | | | | | |
| Affected Version(s): - | | | | | |
| Uncaught Exception | 03-Feb-2025 | 7.5 | In network HW, there is a possible system hang due to an uncaught exception. This could lead to remote denial of service with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT79-170225/322 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00399035; Issue ID: MSV-2380.<br>**CVE ID: CVE-2025-20637** | | |
| **Product: mt8167** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/323 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/324 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/325 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/326 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/327 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/328 |
| Use of | 03-Feb-2025 | 4.3 | In DA, there is a possible | https://corp.me | H-MED-MT81- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Uninitialized Variable | | | read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | diatek.com/product-security-bulletin/February-2025 | 170225/329 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/330 |
| **Product: mt8167s** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/331 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT81-170225/332 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br><br>**CVE ID: CVE-2025-20641** | ry-2025 | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br><br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/333 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br><br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/334 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/335 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/336 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/337 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/338 |

| 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 |
|---|---|---|---|---|---|
| **Product: mt8175** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/339 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/340 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/341 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT81-170225/342 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/343 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/344 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/345 |

| 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 |
|---|---|---|---|---|---|
| | | | interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/346 |
| **Product: mt8185** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/347 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/348 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2058.<br>**CVE ID: CVE-2025-20641** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/349 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/350 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/351 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT81-170225/352 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | bulletin/February-2025 | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/353 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/354 |
| **Product: mt8195** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/355 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/356 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/357 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/358 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/359 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/360 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT81-170225/361 |
| Debug Messages Revealing | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT81-170225/362 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unnecessary Information | | | could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | bulletin/February-2025 | |
| **Product: mt8321** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/363 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/364 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/365 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/366 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/367 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/368 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/369 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/370 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/371 |
| **Product: mt8362a** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 6.6 | In DA, there is a possible | https://corp.me | H-MED-MT83- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | diatek.com/product-security-bulletin/February-2025 | 170225/372 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/373 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/374 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/375 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/376 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/377 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/378 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/379 |
| **Product: mt8365** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/380 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/381 |
| Out-of- | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible | https://corp.me | H-MED-MT83- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | diatek.com/product-security-bulletin/February-2025 | 170225/382 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/383 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/384 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/385 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/386 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/387 |
| **Product: mt8370** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/388 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | | |
| **Product: mt8385** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/389 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/390 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/391 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20641** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/392 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/393 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/394 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT83-170225/395 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | ry-2025 | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/396 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/397 |
| **Product: mt8390** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/398 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | | |
| **Product: mt8395** | | | | | |
| Affected Version(s): - | | | | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/399 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/400 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/401 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/402 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/403 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/404 |
| Out-of- | 03-Feb-2025 | 4.3 | In DA, there is a possible | https://corp.me | H-MED-MT83- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Read | | | out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | diatek.com/product-security-bulletin/February-2025 | 170225/405 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT83-170225/406 |
| **Product: mt8666** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/407 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/408 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/409 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/410 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/411 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/412 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/413 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/414 |
| Debug Messages | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a | https://corp.mediatek.com/pro | H-MED-MT86-170225/415 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Revealing Unnecessary Information | | | missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | duct-security-bulletin/February-2025 | |
| **Product: mt8667** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/416 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/417 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/418 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/419 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/420 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/421 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2070.<br>**CVE ID: CVE-2024-20142** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/422 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/423 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/424 |
| **Product: mt8673** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/425 |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/426 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/427 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/428 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/429 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/430 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/431 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/432 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/433 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/434 |
| **Product: mt8675** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/435 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/436 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/437 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/438 |

| 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 |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/439 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/440 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/441 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/442 |
| **Product: mt8676** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/443 |
| **Product: mt8678** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/444 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/445 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/446 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/447 |
| Write-what- | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible | https://corp.me | H-MED-MT86- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| where Condition | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | diatek.com/product-security-bulletin/February-2025 | 170225/448 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/449 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/450 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/451 |

| 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 |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT86-170225/452 |
| **Product: mt8755** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/453 |
| **Product: mt8765** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/454 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/455 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/456 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/457 |

| 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 |
|---|---|---|---|---|---|
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/458 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/459 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/460 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/461 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/462 |
| **Product: mt8766** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/463 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/464 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/465 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/466 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/467 |
| Write-what- | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible | https://corp.me | H-MED-MT87- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| where Condition | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | diatek.com/product-security-bulletin/February-2025 | 170225/468 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/469 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/470 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/471 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | | |
| **Product: mt8768** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/472 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/473 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/474 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/475 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/476 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/477 |
| Use of Uninitialized | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap | https://corp.mediatek.com/pro | H-MED-MT87-170225/478 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Variable | | | data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/479 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/480 |
| **Product: mt8771** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/481 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/482 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/483 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/484 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2060.<br>**CVE ID: CVE-2025-20639** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/485 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/486 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/487 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized | https://corp.mediatek.com/product-security- | H-MED-MT87-170225/488 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | bulletin/February-2025 | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/489 |
| **Product: mt8775** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/490 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/491 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/492 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/493 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/494 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20642** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/495 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/496 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/497 |
| Debug Messages Revealing Unnecessary | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local | https://corp.mediatek.com/product-security-bulletin/Februa | H-MED-MT87-170225/498 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Information | | | information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | ry-2025 | |
| **Product: mt8781** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/499 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/500 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/501 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/502 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/503 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/504 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-20141** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/505 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/506 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/507 |
| **Product: mt8786** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of- | 03-Feb-2025 | 6.7 | In secmem, there is a | https://corp.me | H-MED-MT87- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | diatek.com/product-security-bulletin/February-2025 | 170225/508 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/509 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/510 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/511 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/512 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/513 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/514 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20638** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/515 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/516 |
| **Product: mt8788** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/517 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | H-MED-MT87-170225/518 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/519 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/520 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/521 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/522 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/523 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/524 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/525 |
| **Product: mt8789** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/526 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/527 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | H-MED-MT87-170225/528 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/529 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/530 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/531 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/532 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/533 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056. | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/534 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20643** | | |
| **Product: mt8791t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/535 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/536 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/537 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | H-MED-MT87-170225/538 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/539 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/540 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/541 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/542 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/543 |
| **Product: mt8795t** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/544 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/545 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/546 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/547 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | H-MED-MT87-170225/548 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/549 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/550 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/551 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/552 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/553 |
| **Product: mt8796** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/554 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2431.<br>**CVE ID: CVE-2025-20636** | | |
| **Product: mt8797** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/555 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/556 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/557 |
| Out-of- | 03-Feb-2025 | 6.6 | In DA, there is a possible | https://corp.me | H-MED-MT87- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| bounds Write | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | diatek.com/product-security-bulletin/February-2025 | 170225/558 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/559 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/560 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/561 |

| 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 |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/562 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/563 |
| **Product: mt8798** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/564 |

| 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 |
|---|---|---|---|---|---|
| | | | needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/565 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/566 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/567 |
| Write-what- | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible | https://corp.me | H-MED-MT87- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| where Condition | | | out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | diatek.com/product-security-bulletin/February-2025 | 170225/568 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/569 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/570 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/571 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | | |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/572 |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT87-170225/573 |
| **Product: mt8863** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/574 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | | |
| **Product: mt8893** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/575 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/576 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/577 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/578 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/579 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/580 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | H-MED-MT88-170225/581 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | bulletin/February-2025 | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | H-MED-MT88-170225/582 |
| **Vendor: Qualcomm** | | | | | |
| **Product: aqt1000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AQT1-170225/583 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AQT1-170225/584 |
| Time-of-check Time-of-use (TOCTOU) Race | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-AQT1-170225/585 |

| 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 |
|---|---|---|---|---|---|
| Condition | | | **CVE ID: CVE-2024-45560** | y-2025-bulletin.html | |
| **Product: ar8035** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/586 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/587 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/588 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/589 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/590 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/591 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in | https://docs.qualcomm.com/product/publicresources/security | H-QUA-AR80-170225/592 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | modem.<br>**CVE ID: CVE-2024-38404** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/593 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-AR80-170225/594 |
| **Product: c-v2x_9150** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-C-V2-170225/595 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-C-V2-170225/596 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-C-V2-170225/597 |
| **Product: csr8811** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSR8-170225/598 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSR8-170225/599 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSR8-170225/600 |
| **Product: csra6620** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSRA-170225/601 |
| **Product: csra6640** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSRA-170225/602 |
| **Product: csrb31024** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-CSRB-170225/603 |
| **Product: fastconnect_6200** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-FAST-170225/604 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/605 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/606 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/607 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/608 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/609 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/610 |
| **Product: fastconnect_6700** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | H-QUA-FAST-170225/611 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/612 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/613 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/614 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/615 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/616 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/617 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-FAST-170225/618 |

| 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-2024-45571** | y-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/619 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/620 |
| **Product: fastconnect_6800** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/621 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/622 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/623 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/624 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-FAST-170225/625 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/626 |
| **Product: fastconnect_6900** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/627 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/628 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/629 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/630 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/631 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera | https://docs.qualcomm.com/product/publicres | H-QUA-FAST-170225/632 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensor.<br>**CVE ID: CVE-2024-49834** | ources/security bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/633 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/634 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/635 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/636 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/637 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/638 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-FAST-170225/639 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45573** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/640 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/641 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/642 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/643 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/644 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/645 |
| **Product: fastconnect_7800** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-FAST-170225/646 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/647 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/648 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/649 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/650 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality. **CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/651 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/652 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-FAST-170225/653 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/654 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/655 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/656 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/657 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/658 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/659 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/660 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | H-QUA-FAST- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pointer Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/661 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/662 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/663 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/664 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/665 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/666 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FAST-170225/667 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. | https://docs.qualcomm.com/product/publicres | H-QUA-FAST-170225/668 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38417** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: flight_rb5_5g_platform** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-FLIG-170225/669 |
| **Product: immersive_home_214** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/670 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/671 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/672 |
| **Product: immersive_home_216** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/673 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | H-QUA-IMME-170225/674 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-IMME-170225/675 |
| **Product: immersive_home_316** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-IMME-170225/676 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-IMME-170225/677 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-IMME-170225/678 |
| **Product: immersive_home_318** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-IMME-170225/679 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025- | H-QUA-IMME-170225/680 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/681 |
| **Product: immersive_home_3210** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/682 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/683 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/684 |
| **Product: immersive_home_326** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/685 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IMME-170225/686 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping | https://docs.qualcomm.com/pr | H-QUA-IMME-170225/687 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: ipq5010** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/688 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/689 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/690 |
| **Product: ipq5028** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/691 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/692 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-IPQ5-170225/693 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | y-2025-bulletin.html | |
| **Product: ipq5300** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/694 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/695 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/696 |
| **Product: ipq5302** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/697 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/698 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/699 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: ipq5312** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/700 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/701 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/702 |
| **Product: ipq5332** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/703 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/704 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ5-170225/705 |
| **Product: ipq6000** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/706 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/707 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/708 |
| **Product: ipq6010** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/709 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/710 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/711 |
| **Product: ipq6018** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | H-QUA-IPQ6-170225/712 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/713 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/714 |
| **Product: ipq6028** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/715 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/716 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ6-170225/717 |
| **Product: ipq8070a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-IPQ8-170225/718 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/719 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/720 |
| **Product: ipq8071a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/721 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/722 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/723 |
| **Product: ipq8072a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/724 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | H-QUA-IPQ8-170225/725 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/726 |
| **Product: ipq8074a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/727 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/728 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/729 |
| **Product: ipq8076** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/730 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-IPQ8-170225/731 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/732 |
| **Product: ipq8076a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/733 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/734 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/735 |
| **Product: ipq8078** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/736 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/737 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-IPQ8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/738 |
| **Product: ipq8078a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/739 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/740 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/741 |
| **Product: ipq8173** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/742 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/743 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command | https://docs.qualcomm.com/product/publicresources/security | H-QUA-IPQ8-170225/744 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the interface.<br>**CVE ID: CVE-2024-45571** | bulletin/februar y-2025-bulletin.html | |
| **Product: ipq8174** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/745 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/746 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ8-170225/747 |
| **Product: ipq9008** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/748 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/749 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/750 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: ipq9048** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/751 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/752 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/753 |
| **Product: ipq9554** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/754 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/755 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/756 |
| **Product: ipq9570** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/757 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/758 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/759 |
| **Product: ipq9574** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/760 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/761 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-IPQ9-170225/762 |
| **Product: mdm9628** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-MDM9-170225/763 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: msm8996au** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-MSM8-170225/764 |
| **Product: qam8255p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/765 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/766 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/767 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/768 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QAM8-170225/769 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/770 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/771 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/772 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/773 |
| **Product: qam8295p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/774 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/775 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QAM8-170225/776 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/777 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/778 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/779 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/780 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/781 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/782 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/783 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qam8620p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/784 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/785 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/786 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/787 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/788 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/789 |
| **Product: qam8650p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | H-QUA-QAM8-170225/790 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/791 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/792 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/793 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/794 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/795 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/796 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QAM8-170225/797 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/798 |
| **Product: qam8775p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/799 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/800 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/801 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/802 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/803 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QAM8-170225/804 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/805 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/806 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAM8-170225/807 |
| **Product: qamsrv1h** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/808 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/809 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/810 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | H-QUA-QAMS-170225/811 |

| 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 |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/812 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/813 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/814 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/815 |
| **Product: qamsrv1m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/816 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QAMS-170225/817 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | H-QUA-QAMS-170225/818 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/819 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/820 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/821 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/822 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QAMS-170225/823 |
| **Product: qca0000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA0-170225/824 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | H-QUA-QCA0- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/825 |
| **Product: qca4024** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA4-170225/826 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA4-170225/827 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA4-170225/828 |
| **Product: qca6174a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/829 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/830 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCA6-170225/831 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/832 |
| **Product: qca6310** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/833 |
| **Product: qca6335** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/834 |
| **Product: qca6391** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/835 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/836 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCA6-170225/837 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/838 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/839 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/840 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/841 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/842 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/843 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCA6-170225/844 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qca6420** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/845 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/846 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/847 |
| **Product: qca6421** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/848 |
| **Product: qca6426** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/849 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCA6-170225/850 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/851 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/852 |
| **Product: qca6430** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/853 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/854 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/855 |
| **Product: qca6431** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/856 |
| **Product: qca6436** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/857 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/858 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/859 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/860 |
| **Product: qca6554a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/861 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/862 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCA6-170225/863 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/864 |
| **Product: qca6564a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/865 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/866 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/867 |
| **Product: qca6564au** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/868 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/869 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Information disclosure | https://docs.qu | H-QUA-QCA6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/870 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/871 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/872 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/873 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/874 |
| **Product: qca6574** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/875 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/876 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/877 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/878 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/879 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/880 |
| **Product: qca6574a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/881 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/882 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCA6-170225/883 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/884 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/885 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/886 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/887 |
| **Product: qca6574au** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/888 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/889 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCA6-170225/890 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/891 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/892 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/893 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/894 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/895 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/896 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/897 |

| 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 |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/898 |
| **Product: qca6584au** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/899 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/900 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/901 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/902 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/903 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCA6-170225/904 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/905 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/906 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/907 |
| **Product: qca6595** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/908 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/909 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/910 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCA6-170225/911 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/912 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/913 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/914 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/915 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/916 |
| **Product: qca6595au** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCA6-170225/917 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicres | H-QUA-QCA6-170225/918 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/919 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/920 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/921 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/922 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/923 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/924 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCA6-170225/925 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/926 |
| **Product: qca6678aq** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/927 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/928 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/929 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/930 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/931 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCA6-170225/932 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | bulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/933 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/934 |
| **Product: qca6688aq** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/935 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/936 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/937 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/938 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | H-QUA-QCA6-170225/939 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qca6696** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/940 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/941 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/942 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/943 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/944 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/945 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | H-QUA-QCA6-170225/946 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/947 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/948 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/949 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/950 |
| **Product: qca6698aq** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/951 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/952 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Information disclosure | https://docs.qu | H-QUA-QCA6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/953 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/954 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/955 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/956 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/957 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/958 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/959 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect | https://docs.qualcomm.com/product/publicres | H-QUA-QCA6-170225/960 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/961 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/962 |
| **Product: qca6777aq** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/963 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/964 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/965 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/966 |
| **Product: qca6787aq** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/967 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/968 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/969 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/970 |
| **Product: qca6797aq** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/971 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/972 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCA6-170225/973 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/974 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/975 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/976 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/977 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA6-170225/978 |
| **Product: qca8075** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/979 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | H-QUA-QCA8-170225/980 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/981 |
| **Product: qca8081** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/982 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/983 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/984 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/985 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | H-QUA-QCA8-170225/986 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | H-QUA-QCA8-170225/987 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Dereference | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/988 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/989 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/990 |
| **Product: qca8082** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/991 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/992 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/993 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qca8084** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/994 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/995 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/996 |
| **Product: qca8085** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/997 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/998 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/999 |
| **Product: qca8337** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1000 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1001 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1002 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1003 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1004 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1005 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1006 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control | https://docs.qualcomm.com/pr | H-QUA-QCA8-170225/1007 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands.<br>**CVE ID: CVE-2024-38417** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1008 |
| **Product: qca8386** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1009 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1010 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA8-170225/1011 |
| **Product: qca9367** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1012 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCA9-170225/1013 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1014 |
| **Product: qca9377** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1015 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1016 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1017 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1018 |
| **Product: qca9888** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1019 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | H-QUA-QCA9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1020 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1021 |
| **Product: qca9889** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1022 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1023 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCA9-170225/1024 |
| **Product: qcc2073** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1025 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCC2-170225/1026 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1027 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1028 |
| **Product: qcc2076** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1029 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1030 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1031 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC2-170225/1032 |
| **Product: qcc710** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1033 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1034 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1035 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1036 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1037 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1038 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1039 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control | https://docs.qualcomm.com/pr | H-QUA-QCC7-170225/1040 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands.<br>**CVE ID: CVE-2024-38417** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCC7-170225/1041 |
| **Product: qcf8000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1042 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1043 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1044 |
| **Product: qcf8000sfp** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1045 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCF8-170225/1046 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1047 |
| **Product: qcf8001** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1048 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1049 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCF8-170225/1050 |
| **Product: qcm4325** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM4-170225/1051 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM4-170225/1052 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qcm4490** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM4-170225/1053 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM4-170225/1054 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM4-170225/1055 |
| **Product: qcm5430** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1056 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1057 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1058 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-QCM5-170225/1059 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1060 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1061 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1062 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM5-170225/1063 |
| **Product: qcm6125** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1064 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1065 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | H-QUA-QCM6-170225/1066 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: qcm6490** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1067 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1068 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1069 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1070 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1071 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1072 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-QCM6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1073 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM6-170225/1074 |
| **Product: qcm8550** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1075 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1076 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1077 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1078 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1079 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1080 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1081 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1082 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1083 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls. **CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCM8-170225/1084 |
| **Product: qcn5022** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1085 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCN5-170225/1086 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1087 |
| **Product: qcn5024** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1088 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1089 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1090 |
| **Product: qcn5052** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1091 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1092 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping | https://docs.qualcomm.com/pr | H-QUA-QCN5-170225/1093 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: qcn5122** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1094 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1095 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1096 |
| **Product: qcn5124** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1097 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1098 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCN5-170225/1099 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | y-2025-bulletin.html | |
| **Product: qcn5152** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1100 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1101 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1102 |
| **Product: qcn5154** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1103 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1104 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1105 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qcn5164** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1106 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1107 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN5-170225/1108 |
| **Product: qcn6023** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1109 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1110 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1111 |
| **Product: qcn6024** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1112 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1113 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1114 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1115 |
| **Product: qcn6112** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1116 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1117 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCN6-170225/1118 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| **Product: qcn6122** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1119 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1120 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1121 |
| **Product: qcn6132** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1122 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1123 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1124 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qcn6224** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1125 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1126 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1127 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1128 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1129 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1130 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCN6-170225/1131 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38404** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1132 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1133 |
| **Product: qcn6274** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1134 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1135 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1136 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1137 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCN6-170225/1138 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1139 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1140 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1141 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1142 |
| **Product: qcn6402** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1143 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1144 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after | https://docs.qualcomm.com/product/publicres | H-QUA-QCN6-170225/1145 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qcn6412** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1146 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1147 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1148 |
| **Product: qcn6422** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1149 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1150 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCN6-170225/1151 |

| 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-2024-45571** | bulletin.html | |
| **Product: qcn6432** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1152 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1153 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN6-170225/1154 |
| **Product: qcn9000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1155 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1156 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1157 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qcn9011** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1158 |
| **Product: qcn9012** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1159 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1160 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1161 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1162 |
| **Product: qcn9022** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1163 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1164 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1165 |
| **Product: qcn9024** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1166 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1167 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1168 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1169 |
| **Product: qcn9070** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | H-QUA-QCN9-170225/1170 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1171 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1172 |
| **Product: qcn9072** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1173 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1174 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1175 |
| **Product: qcn9074** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCN9-170225/1176 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1177 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1178 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1179 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1180 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1181 |
| **Product: qcn9100** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1182 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCN9-170225/1183 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1184 |
| **Product: qcn9160** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1185 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1186 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1187 |
| **Product: qcn9274** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1188 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1189 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | H-QUA-QCN9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1190 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1191 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1192 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCN9-170225/1193 |
| **Product: qcs410** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1194 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1195 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1196 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1197 |
| **Product: qcs4490** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1198 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1199 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS4-170225/1200 |
| **Product: qcs5430** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS5-170225/1201 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS5-170225/1202 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-QCS5-170225/1203 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS5-170225/1204 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS5-170225/1205 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS5-170225/1206 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS5-170225/1207 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS5-170225/1208 |
| **Product: qcs610** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QCS6-170225/1209 |
| Time-of-check Time- | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map | https://docs.qualcomm.com/pr | H-QUA-QCS6-170225/1210 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of-use (TOCTOU) Race Condition | | | info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1211 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1212 |
| **Product: qcs6125** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1213 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1214 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1215 |
| **Product: qcs615** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QCS6-170225/1216 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1217 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1218 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1219 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1220 |
| **Product: qcs6490** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1221 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1222 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QCS6-170225/1223 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1224 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1225 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1226 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1227 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1228 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1229 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCS6-170225/1230 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1231 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS6-170225/1232 |
| **Product: qcs7230** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS7-170225/1233 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS7-170225/1234 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS7-170225/1235 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS7-170225/1236 |
| **Product: qcs8250** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | H-QUA-QCS8-170225/1237 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1238 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1239 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1240 |
| **Product: qcs8300** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1241 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1242 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1243 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | H-QUA-QCS8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1244 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1245 |
| **Product: qcs8550** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1246 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1247 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1248 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1249 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1250 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1251 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1252 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1253 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls. **CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1254 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS8-170225/1255 |
| **Product: qcs9100** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS9-170225/1256 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QCS9-170225/1257 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS9-170225/1258 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS9-170225/1259 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS9-170225/1260 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QCS9-170225/1261 |
| **Product: qdu1000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1262 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1263 |
| **Product: qdu1010** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | H-QUA-QDU1-170225/1264 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1265 |
| **Product: qdu1110** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1266 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1267 |
| **Product: qdu1210** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1268 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDU1-170225/1269 |
| **Product: qdx1010** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | H-QUA-QDX1-170225/1270 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDX1-170225/1271 |
| **Product: qdx1011** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDX1-170225/1272 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QDX1-170225/1273 |
| **Product: qep8111** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QEP8-170225/1274 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QEP8-170225/1275 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-QEP8-170225/1276 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | y-2025-bulletin.html | |
| **Product: qfw7114** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1277 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1278 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1279 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1280 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1281 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1282 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in | https://docs.qualcomm.com/product/publicresources/security | H-QUA-QFW7-170225/1283 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | modem.<br>**CVE ID: CVE-2024-38404** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1284 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1285 |
| **Product: qfw7124** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1286 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1287 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1288 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QFW7-170225/1289 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after | https://docs.qualcomm.com/product/publicres | H-QUA-QFW7-170225/1290 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | ources/security bulletin/februar y-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QFW7-170225/1291 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QFW7-170225/1292 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QFW7-170225/1293 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QFW7-170225/1294 |
| **Product: qrb5165m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-QRB5-170225/1295 |
| **Product: qrb5165n** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025- | H-QUA-QRB5-170225/1296 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| **Product: qru1032** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QRU1-170225/1297 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QRU1-170225/1298 |
| **Product: qru1052** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QRU1-170225/1299 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QRU1-170225/1300 |
| **Product: qru1062** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QRU1-170225/1301 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QRU1-170225/1302 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| **Product: qsm8250** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QSM8-170225/1303 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QSM8-170225/1304 |
| **Product: qsm8350** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QSM8-170225/1305 |
| **Product: qxm8083** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QXM8-170225/1306 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-QXM8-170225/1307 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-QXM8-170225/1308 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| **Product: robotics_rb2** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-ROBO-170225/1309 |
| **Product: robotics_rb3** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-ROBO-170225/1310 |
| **Product: robotics_rb5** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-ROBO-170225/1311 |
| **Product: sa6145p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1312 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1313 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | H-QUA-SA61- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1314 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1315 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1316 |
| **Product: sa6150p** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1317 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1318 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1319 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1320 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sa6155** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1321 |
| **Product: sa6155p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1322 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1323 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1324 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1325 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1326 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | H-QUA-SA61-170225/1327 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1328 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1329 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1330 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA61-170225/1331 |
| **Product: sa7255p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1332 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1333 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | H-QUA-SA72-170225/1334 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1335 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1336 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1337 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1338 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA72-170225/1339 |
| **Product: sa7775p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1340 |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | H-QUA-SA77- |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1341 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1342 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1343 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1344 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1345 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1346 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA77-170225/1347 |
| **Product: sa8145p** | | | | | |
| 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 |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1348 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1349 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1350 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization. **CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1351 |
| **Product: sa8150p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1352 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1353 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SA81-170225/1354 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38414** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1355 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1356 |
| **Product: sa8155** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1357 |
| **Product: sa8155p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1358 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1359 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1360 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Information disclosure | https://docs.qu | H-QUA-SA81- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1361 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1362 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1363 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1364 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1365 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1366 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1367 |
| **Product: sa8195p** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1368 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1369 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1370 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1371 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1372 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1373 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization. **CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1374 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control | https://docs.qualcomm.com/pr | H-QUA-SA81-170225/1375 |

| 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 |
|---|---|---|---|---|---|
| | | | commands.<br>**CVE ID: CVE-2024-38417** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA81-170225/1376 |
| **Product: sa8255p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1377 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1378 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1379 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1380 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1381 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | H-QUA-SA82- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1382 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1383 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1384 |
| **Product: sa8295p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1385 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1386 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1387 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1388 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1389 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1390 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1391 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1392 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1393 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA82-170225/1394 |
| **Product: sa8530p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SA85-170225/1395 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1396 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1397 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1398 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1399 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1400 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1401 |
| **Product: sa8540p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SA85-170225/1402 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1403 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1404 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1405 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1406 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1407 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1408 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1409 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA85-170225/1410 |
| **Product: sa8620p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1411 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1412 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1413 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1414 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1415 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SA86-170225/1416 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1417 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1418 |
| **Product: sa8650p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1419 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1420 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1421 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1422 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SA86-170225/1423 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1424 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1425 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA86-170225/1426 |
| **Product: sa8770p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1427 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1428 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1429 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SA87-170225/1430 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1431 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1432 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1433 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1434 |
| **Product: sa8775p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1435 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1436 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-SA87-170225/1437 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1438 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1439 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1440 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1441 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA87-170225/1442 |
| **Product: sa9000p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1443 |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | H-QUA-SA90-170225/1444 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1445 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1446 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1447 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1448 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1449 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1450 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SA90-170225/1451 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1452 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1453 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SA90-170225/1454 |
| **Product: sc8180x-aaab** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1455 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1456 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1457 |
| **Product: sc8180x-acaf** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1458 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1459 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1460 |
| **Product: sc8180x-ad** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1461 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1462 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1463 |
| **Product: sc8180xp-aaab** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicres | H-QUA-SC81-170225/1464 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: sc8180xp-acaf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1465 |
| **Product: sc8180xp-ad** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC81-170225/1466 |
| **Product: sc8280xp-abbb** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC82-170225/1467 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC82-170225/1468 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC82-170225/1469 |
| Use of Out-of-range Pointer | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative | https://docs.qualcomm.com/product/publicres | H-QUA-SC82-170225/1470 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Offset | | | indexing of display ID.<br>**CVE ID: CVE-2024-45573** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: sc8380xp** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1471 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1472 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1473 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1474 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1475 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SC83-170225/1476 |
| **Product: sd670** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD67-170225/1477 |
| **Product: sd675** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD67-170225/1478 |
| **Product: sd855** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD85-170225/1479 |
| **Product: sd865_5g** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD86-170225/1480 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD86-170225/1481 |
| Time-of-check Time-of-use (TOCTOU) Race | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SD86-170225/1482 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Condition | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD86-170225/1483 |
| **Product: sd888** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD88-170225/1484 |
| **Product: sdm429w** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1485 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1486 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1487 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1488 |
| Use of Out- | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-SDM4- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of-range Pointer Offset | | | occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1489 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1490 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1491 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDM4-170225/1492 |
| **Product: sdx55** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1493 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1494 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1495 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1496 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1497 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1498 |
| **Product: sdx57m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX5-170225/1499 |
| **Product: sdx61** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX6-170225/1500 |
| **Product: sdx65m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX6-170225/1501 |

| 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 |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX6-170225/1502 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX6-170225/1503 |
| **Product: sdx80m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX8-170225/1504 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SDX8-170225/1505 |
| **Product: sd_675** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_6-170225/1506 |
| **Product: sd_8cx** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_8-170225/1507 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: sd_8_gen1_5g** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_8-170225/1508 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_8-170225/1509 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_8-170225/1510 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SD_8-170225/1511 |
| **Product: sg4150p** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG41-170225/1512 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG41-170225/1513 |
| **Product: sg8275p** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG82-170225/1514 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG82-170225/1515 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG82-170225/1516 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SG82-170225/1517 |
| **Product: sm4635** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM46-170225/1518 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM46-170225/1519 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SM46-170225/1520 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM46-170225/1521 |
| **Product: sm6370** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM63-170225/1522 |
| **Product: sm6650** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1523 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1524 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1525 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1526 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down | https://docs.qualcomm.com/pr | H-QUA-SM66-170225/1527 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1528 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1529 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1530 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM66-170225/1531 |
| **Product: sm7250p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM72-170225/1532 |
| **Product: sm7315** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SM73-170225/1533 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | y-2025-bulletin.html | |
| **Product: sm7325p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM73-170225/1534 |
| **Product: sm7635** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1535 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1536 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1537 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1538 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1539 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | H-QUA-SM76- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1540 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1541 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1542 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1543 |
| **Product: sm7675** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1544 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1545 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1546 |

| 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 |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1547 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1548 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1549 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1550 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1551 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1552 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1553 |
| **Product: sm7675p** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1554 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1555 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1556 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1557 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1558 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1559 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1560 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-SM76- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1561 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1562 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM76-170225/1563 |
| **Product: sm8550p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1564 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1565 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1566 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1567 |

| 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 |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1568 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1569 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1570 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM85-170225/1571 |
| **Product: sm8635** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1572 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1573 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SM86-170225/1574 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1575 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1576 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1577 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1578 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1579 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1580 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1581 |
| **Product: sm8635p** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1582 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1583 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1584 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1585 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1586 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1587 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1588 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | H-QUA-SM86- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1589 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1590 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM86-170225/1591 |
| **Product: sm8750** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1592 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1593 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1594 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1595 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1596 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1597 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1598 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1599 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1600 |
| **Product: sm8750p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1601 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SM87-170225/1602 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1603 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1604 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1605 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1606 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1607 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1608 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SM87-170225/1609 |
| **Product: smart_audio_400** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SMAR-170225/1610 |
| **Product: snapdragon_429_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1611 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1612 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1613 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1614 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1615 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1616 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1617 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1618 |
| **Product: snapdragon_460_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1619 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1620 |
| **Product: snapdragon_480\+_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1621 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1622 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1623 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1624 |
| **Product: snapdragon_480_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1625 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1626 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1627 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1628 |
| **Product: snapdragon_4_gen_1_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-SNAP-170225/1629 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1630 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1631 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1632 |
| **Product: snapdragon_4_gen_2_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1633 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1634 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1635 |
| **Product: snapdragon_662_mobile** | | | | | |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1636 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1637 |
| **Product: snapdragon_670_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1638 |
| **Product: snapdragon_675_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1639 |
| **Product: snapdragon_678_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1640 |
| **Product: snapdragon_680_4g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | H-QUA-SNAP-170225/1641 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | with invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1642 |
| **Product: snapdragon_685_4g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1643 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1644 |
| **Product: snapdragon_695_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1645 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1646 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1647 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49843** | y-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1648 |
| **Product: snapdragon_765g_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1649 |
| **Product: snapdragon_765_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1650 |
| **Product: snapdragon_768g_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1651 |
| **Product: snapdragon_778g\+_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1652 |
| **Product: snapdragon_778g_5g_mobile** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1653 |
| **Product: snapdragon_780g_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1654 |
| **Product: snapdragon_782g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1655 |
| **Product: snapdragon_7c\+_gen_3_compute** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1656 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1657 |
| Time-of-check Time-of-use (TOCTOU) Race | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1658 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Condition | | | **CVE ID: CVE-2024-45560** | y-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. **CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1659 |
| **Product: snapdragon_820_automotive** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1660 |
| **Product: snapdragon_845_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1661 |
| **Product: snapdragon_850_mobile_compute** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1662 |
| **Product: snapdragon_855\+_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1663 |
| **Product: snapdragon_855_mobile** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1664 |
| **Product: snapdragon_860_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1665 |
| **Product: snapdragon_865\+_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1666 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1667 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1668 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1669 |
| **Product: snapdragon_865_5g_mobile** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1670 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1671 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1672 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1673 |
| **Product: snapdragon_870_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1674 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1675 |
| Time-of-check Time-of-use (TOCTOU) Race | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1676 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Condition | | | **CVE ID: CVE-2024-38418** | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1677 |
| **Product: snapdragon_888\+_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1678 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1679 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1680 |
| **Product: snapdragon_888_5g_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1681 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1682 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | H-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1683 |
| **Product: snapdragon_8\+_gen_1_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1684 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1685 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1686 |
| **Product: snapdragon_8\+_gen_2_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1687 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1688 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1689 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1690 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1691 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1692 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1693 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1694 |
| **Product: snapdragon_8_gen_1_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1695 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-SNAP-170225/1696 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1697 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1698 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1699 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1700 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1701 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1702 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1703 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| **Product: snapdragon_8_gen_2_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1704 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1705 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1706 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1707 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1708 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1709 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1710 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1711 |
| **Product: snapdragon_8_gen_3_mobile** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1712 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1713 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1714 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1715 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1716 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB | https://docs.qualcomm.com/product/publicres | H-QUA-SNAP-170225/1717 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bus error.<br>**CVE ID: CVE-2024-49843** | ources/security bulletin/februar y-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1718 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1719 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1720 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1721 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1722 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-SNAP-170225/1723 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1724 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38411** | y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1725 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1726 |
| **Product: snapdragon_ar1_gen_1** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1727 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1728 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1729 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1730 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1731 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | bulletin/february-2025-bulletin.html | |
| **Product: snapdragon_ar2_gen_1** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1732 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1733 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1734 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1735 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1736 |
| **Product: snapdragon_auto_4g_modem** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1737 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: snapdragon_auto_5g_modem-rf_gen_2** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1738 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1739 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1740 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1741 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1742 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1743 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SNAP-170225/1744 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1745 |
| **Product: snapdragon_w5\+_gen_1_wearable** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1746 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1747 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1748 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1749 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1750 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SNAP-170225/1751 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38414** | y-2025-bulletin.html | |
| **Product: snapdragon_wear_4100\+** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1752 |
| **Product: snapdragon_x24_lte_modem** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1753 |
| **Product: snapdragon_x35_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1754 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1755 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1756 |
| **Product: snapdragon_x50_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | H-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1757 |
| **Product: snapdragon_x55_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1758 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1759 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1760 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1761 |
| **Product: snapdragon_x62_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1762 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1763 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| **Product: snapdragon_x65_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1764 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1765 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1766 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1767 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1768 |
| **Product: snapdragon_x72_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1769 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1770 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1771 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1772 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1773 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1774 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1775 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1776 |
| **Product: snapdragon_x72_5g_modem-rf_system** | | | | | |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1777 |
| **Product: snapdragon_x75_5g_modem-rf** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1778 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1779 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1780 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1781 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1782 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1783 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the interface.<br>**CVE ID: CVE-2024-45571** | bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1784 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1785 |
| **Product: snapdragon_x75_5g_modem-rf_system** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1786 |
| **Product: snapdragon_xr2\+_gen_1** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1787 |
| **Product: snapdragon_xr2_5g** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1788 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SNAP-170225/1789 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1790 |
| **Product: snapdragon_xr2_5g_platform** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SNAP-170225/1791 |
| **Product: srv1h** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1792 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1793 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1794 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1795 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1796 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1797 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1798 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1799 |
| **Product: srv1l** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1800 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1801 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-SRV1-170225/1802 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1803 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1804 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1805 |
| **Product: srv1m** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1806 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1807 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1808 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-SRV1-170225/1809 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1810 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1811 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1812 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SRV1-170225/1813 |
| **Product: ssg2115p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1814 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1815 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SSG2-170225/1816 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1817 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1818 |
| **Product: ssg2125p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1819 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1820 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1821 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SSG2-170225/1822 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicres | H-QUA-SSG2-170225/1823 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: sw5100** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1824 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1825 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1826 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1827 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1828 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1829 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing | https://docs.qualcomm.com/pr | H-QUA-SW51-170225/1830 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: sw5100p** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1831 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1832 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1833 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1834 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1835 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SW51-170225/1836 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | H-QUA-SW51- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1837 |
| **Product: sxr1230p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR1-170225/1838 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR1-170225/1839 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR1-170225/1840 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR1-170225/1841 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR1-170225/1842 |
| **Product: sxr2130** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-SXR2-170225/1843 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1844 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1845 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1846 |
| **Product: sxr2230p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1847 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1848 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1849 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera | https://docs.qualcomm.com/product/publicres | H-QUA-SXR2-170225/1850 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensor.<br>**CVE ID: CVE-2024-49834** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1851 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1852 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1853 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1854 |
| **Product: sxr2250p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1855 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1856 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | H-QUA-SXR2-170225/1857 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1858 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1859 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1860 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1861 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1862 |
| **Product: sxr2330p** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1863 |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | H-QUA-SXR2- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1864 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1865 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1866 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1867 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1868 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1869 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-SXR2-170225/1870 |
| **Product: talynplus** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-TALY-170225/1871 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-TALY-170225/1872 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-TALY-170225/1873 |
| **Product: video_collaboration_vc1_platform** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1874 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1875 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1876 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-VIDE-170225/1877 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1878 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1879 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1880 |
| **Product: video_collaboration_vc3** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1881 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1882 |
| **Product: video_collaboration_vc3_platform** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1883 |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | H-QUA-VIDE-170225/1884 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1885 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1886 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1887 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1888 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1889 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1890 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . | https://docs.qualcomm.com/product/publicresources/security | H-QUA-VIDE-170225/1891 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45582** | bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1892 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1893 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1894 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1895 |
| **Product: video_collaboration_vc5** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1896 |
| **Product: video_collaboration_vc5_platform** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1897 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1898 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VIDE-170225/1899 |
| **Product: vision_intelligence_300** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VISI-170225/1900 |
| **Product: vision_intelligence_400** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VISI-170225/1901 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VISI-170225/1902 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-VISI-170225/1903 |
| **Product: wcd9326** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1904 |
| **Product: wcd9335** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1905 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1906 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1907 |
| **Product: wcd9340** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1908 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1909 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | H-QUA-WCD9-170225/1910 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1911 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1912 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1913 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1914 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1915 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCD9-170225/1916 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCD9-170225/1917 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1918 |
| **Product: wcd9341** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1919 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1920 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1921 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1922 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1923 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCD9-170225/1924 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1925 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1926 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1927 |
| **Product: wcd9370** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1928 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1929 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1930 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | H-QUA-WCD9-170225/1931 |

| 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 |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1932 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1933 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1934 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1935 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1936 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1937 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCD9-170225/1938 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45573** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1939 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1940 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1941 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1942 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1943 |
| **Product: wcd9375** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1944 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCD9-170225/1945 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1946 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1947 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1948 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1949 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1950 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1951 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WCD9-170225/1952 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1953 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1954 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1955 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1956 |
| **Product: wcd9378** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1957 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1958 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCD9-170225/1959 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1960 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1961 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1962 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1963 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1964 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1965 |
| **Product: wcd9380** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCD9-170225/1966 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1967 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1968 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1969 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1970 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1971 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1972 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WCD9-170225/1973 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45560** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1974 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1975 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1976 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1977 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1978 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1979 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1980 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1981 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1982 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1983 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1984 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1985 |
| **Product: wcd9385** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1986 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WCD9-170225/1987 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1988 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1989 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1990 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1991 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1992 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1993 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1994 |
| Buffer Over- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | H-QUA-WCD9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/1995 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1996 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1997 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1998 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/1999 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2000 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2001 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware | https://docs.qualcomm.com/product/publicres | H-QUA-WCD9-170225/2002 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | image during core initialization.<br>**CVE ID: CVE-2024-38414** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2003 |
| **Product: wcd9390** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2004 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2005 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2006 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2007 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2008 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user | https://docs.qualcomm.com/pr | H-QUA-WCD9-170225/2009 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2010 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2011 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2012 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2013 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2014 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2015 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCD9-170225/2016 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38411** | bulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2017 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2018 |
| **Product: wcd9395** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2019 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2020 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2021 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2022 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera | https://docs.qualcomm.com/product/publicres | H-QUA-WCD9-170225/2023 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensor.<br>**CVE ID: CVE-2024-49834** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2024 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2025 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2026 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2027 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2028 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2029 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCD9-170225/2030 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38404** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2031 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2032 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCD9-170225/2033 |
| **Product: wcn3610** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2034 |
| **Product: wcn3620** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2035 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2036 |
| Buffer Over- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | H-QUA-WCN3- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2037 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2038 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2039 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2040 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2041 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2042 |
| **Product: wcn3660b** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2043 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2044 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2045 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2046 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2047 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2048 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2049 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2050 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control | https://docs.qualcomm.com/pr | H-QUA-WCN3-170225/2051 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | commands.<br>**CVE ID: CVE-2024-38417** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: wcn3680b** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2052 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2053 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2054 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2055 |
| **Product: wcn3950** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2056 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCN3-170225/2057 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2058 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2059 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2060 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2061 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2062 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2063 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2064 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: wcn3980** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2065 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2066 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2067 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2068 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2069 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2070 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WCN3-170225/2071 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38404** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2072 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2073 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2074 |
| **Product: wcn3988** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2075 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2076 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2077 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCN3-170225/2078 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2079 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2080 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2081 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2082 |
| **Product: wcn3990** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2083 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN3-170225/2084 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | H-QUA-WCN3-170225/2085 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: wcn6450** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2086 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2087 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2088 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2089 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2090 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2091 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping | https://docs.qualcomm.com/pr | H-QUA-WCN6-170225/2092 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: wcn6650** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2093 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2094 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2095 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2096 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2097 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2098 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-WCN6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2099 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2100 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2101 |
| **Product: wcn6740** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2102 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2103 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2104 |
| **Product: wcn6755** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCN6-170225/2105 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2106 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2107 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2108 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2109 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2110 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2111 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WCN6-170225/2112 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2113 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN6-170225/2114 |
| **Product: wcn7860** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2115 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2116 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2117 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2118 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCN7-170225/2119 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2120 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2121 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2122 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2123 |
| **Product: wcn7861** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2124 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2125 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | H-QUA-WCN7-170225/2126 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2127 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2128 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2129 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2130 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2131 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WCN7-170225/2132 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WCN7-170225/2133 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49832** | y-2025-bulletin.html | |
| **Product: wcn7880** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2134 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2135 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2136 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2137 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2138 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2139 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WCN7-170225/2140 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49832** | bulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2141 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2142 |
| **Product: wcn7881** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2143 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2144 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2145 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2146 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB | https://docs.qualcomm.com/product/publicres | H-QUA-WCN7-170225/2147 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bus error.<br>**CVE ID: CVE-2024-49843** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2148 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2149 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2150 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2151 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WCN7-170225/2152 |
| **Product: wsa8810** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2153 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | H-QUA-WSA8-170225/2154 |

| 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 |
|---|---|---|---|---|---|
| | | | with invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2155 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2156 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2157 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2158 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2159 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2160 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WSA8-170225/2161 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2162 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2163 |
| **Product: wsa8815** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2164 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2165 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2166 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2167 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera | https://docs.qualcomm.com/product/publicres | H-QUA-WSA8-170225/2168 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | sensor.<br>**CVE ID: CVE-2024-49834** | ources/security bulletin/februar y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2169 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2170 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2171 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2172 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2173 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2174 |
| **Product: wsa8830** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to | https://docs.qualcomm.com/pr | H-QUA-WSA8-170225/2175 |

| 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 |
|---|---|---|---|---|---|
| Array Index | | | invalid frame content.<br>**CVE ID: CVE-2024-45569** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2176 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2177 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2178 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2179 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2180 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2181 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WSA8-170225/2182 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | buffer.<br>**CVE ID: CVE-2024-45560** | bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2183 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2184 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2185 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2186 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2187 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2188 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WSA8-170225/2189 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2190 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2191 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2192 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2193 |
| **Product: wsa8832** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2194 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2195 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WSA8-170225/2196 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2197 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2198 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2199 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2200 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2201 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2202 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2203 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2204 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2205 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2206 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2207 |
| **Product: wsa8835** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2208 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2209 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WSA8-170225/2210 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2211 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2212 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2213 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2214 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2215 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2216 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2217 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | H-QUA-WSA8- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2218 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2219 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2220 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2221 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2222 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2223 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2224 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. | https://docs.qualcomm.com/product/publicres | H-QUA-WSA8-170225/2225 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38417** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2226 |
| **Product: wsa8840** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2227 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2228 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2229 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2230 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2231 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user | https://docs.qualcomm.com/pr | H-QUA-WSA8-170225/2232 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2233 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2234 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2235 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2236 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2237 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2238 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command | https://docs.qualcomm.com/product/publicresources/security | H-QUA-WSA8-170225/2239 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the interface.<br>**CVE ID: CVE-2024-45571** | bulletin/februar y-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2240 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2241 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2242 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2243 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2244 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | H-QUA-WSA8-170225/2245 |
| **Product: wsa8845** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | H-QUA-WSA8-170225/2246 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2247 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2248 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2249 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality. **CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2250 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2251 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2252 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | H-QUA-WSA8-170225/2253 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2254 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2255 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2256 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2257 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2258 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2259 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2260 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2261 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2262 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2263 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2264 |
| **Product: wsa8845h** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2265 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2266 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | H-QUA-WSA8-170225/2267 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2268 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2269 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2270 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2271 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2272 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2273 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2274 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption in | https://docs.qu | H-QUA-WSA8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2275 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2276 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2277 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2278 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2279 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2280 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2281 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets. | https://docs.qualcomm.com/product/publicres | H-QUA-WSA8-170225/2282 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38413** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | H-QUA-WSA8-170225/2283 |
| **Vendor: Zyxel** | | | | | |
| **Product: sbg3300-n000** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-SBG3-170225/2284 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-SBG3-170225/2285 |
| **Product: sbg3300-nb00** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request. **CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-SBG3-170225/2286 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. **CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-SBG3-170225/2287 |
| **Product: sbg3500-nb00** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain- | H-ZYX-SBG3-170225/2288 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-SBG3-170225/2289 |
| **Product: vmg1312-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG1-170225/2290 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities- | H-ZYX-VMG1-170225/2291 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | in-certain-legacy-dsl-cpe-02-04-2025 | |
| **Product: vmg1312-b10b** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG1-170225/2292 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG1-170225/2293 |
| **Product: vmg1312-b10e** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command- | H-ZYX-VMG1-170225/2294 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG1-170225/2295 |
| **Product: vmg3312-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG3-170225/2296 |
| Improper Neutralization of Special Elements used in an OS | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security- | H-ZYX-VMG3-170225/2297 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command ('OS Command Injection') | | | the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| **Product: vmg3313-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG3-170225/2298 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG3-170225/2299 |
| **Product: vmg3926-b10b** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralizati | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** | https://www.zyxel.com/global/ | H-ZYX-VMG3-170225/2300 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Special Elements used in an OS Command ('OS Command Injection') | | | A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG3-170225/2301 |
| **Product: vmg4325-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG4-170225/2302 |
| Improper | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN | https://www.zy | H-ZYX-VMG4- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | | ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | xel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | 170225/2303 |
| **Product: vmg4380-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG4-170225/2304 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe- | H-ZYX-VMG4-170225/2305 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-40891** | 02-04-2025 | |
| **Product: vmg8324-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. **CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG8-170225/2306 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request. **CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG8-170225/2307 |
| **Product: vmg8924-b10a** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure- | H-ZYX-VMG8-170225/2308 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | H-ZYX-VMG8-170225/2309 |
| **Operating System** | | | | | |
| **Vendor: Apple** | | | | | |
| **Product: ipados** | | | | | |
| Affected Version(s): * Up to (excluding) 17.7.5 | | | | | |
| Incorrect Authorization | 10-Feb-2025 | 6.1 | An authorization issue was addressed with improved state management. This issue is fixed in iPadOS 17.7.5, iOS 18.3.1 and iPadOS 18.3.1. A physical attack may disable USB Restricted Mode on a locked device. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.<br>**CVE ID: CVE-2025-24200** | https://support.apple.com/en-us/122173, https://support.apple.com/en-us/122174 | O-APP-IPAD-170225/2310 |
| Affected Version(s): From (including) 18.0 Up to (excluding) 18.3.1 | | | | | |
| Incorrect Authorization | 10-Feb-2025 | 6.1 | An authorization issue was addressed with improved state management. This issue is fixed in iPadOS | https://support.apple.com/en-us/122173, https://support. | O-APP-IPAD-170225/2311 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | 17.7.5, iOS 18.3.1 and iPadOS 18.3.1. A physical attack may disable USB Restricted Mode on a locked device. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.<br>**CVE ID: CVE-2025-24200** | apple.com/en-us/122174 | |
| **Product: iphone_os** | | | | | |
| Affected Version(s): * Up to (excluding) 18.3.1 | | | | | |
| Incorrect Authorization | 10-Feb-2025 | 6.1 | An authorization issue was addressed with improved state management. This issue is fixed in iPadOS 17.7.5, iOS 18.3.1 and iPadOS 18.3.1. A physical attack may disable USB Restricted Mode on a locked device. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.<br>**CVE ID: CVE-2025-24200** | https://support.apple.com/en-us/122173, https://support.apple.com/en-us/122174 | O-APP-IPHO-170225/2312 |
| **Vendor: Dell** | | | | | |
| **Product: data_domain_operating_system** | | | | | |
| Affected Version(s): From (including) 7.10.1.0 Up to (excluding) 7.10.1.50 | | | | | |
| Insufficient Granularity of Access Control | 01-Feb-2025 | 7.8 | Dell PowerProtect DD versions prior to 8.3.0.0, 7.10.1.50, and 7.13.1.20 contain an improper access control vulnerability. A local malicious user with low privileges could potentially exploit this vulnerability leading to escalation of privilege.<br>**CVE ID: CVE-2024-53295** | https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities | O-DEL-DATA-170225/2313 |
| Use of a Risky Cryptograph | 04-Feb-2025 | 3.7 | Dell PowerProtect DD, versions prior to DDOS 8.3.0.0, 7.10.1.50, and | https://www.dell.com/support/kbdoc/en- | O-DEL-DATA-170225/2314 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ic Primitive | | | 7.13.1.10 contains a use of a Cryptographic Primitive with a Risky Implementation vulnerability. A remote attacker could potentially exploit this vulnerability, leading to Information tampering.<br><br>**CVE ID: CVE-2025-22475** | us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities | |
| Affected Version(s): From (including) 7.13.1.0 Up to (excluding) 7.13.1.10 | | | | | |
| Use of a Risky Cryptographic Primitive | 04-Feb-2025 | 3.7 | Dell PowerProtect DD, versions prior to DDOS 8.3.0.0, 7.10.1.50, and 7.13.1.10 contains a use of a Cryptographic Primitive with a Risky Implementation vulnerability. A remote attacker could potentially exploit this vulnerability, leading to Information tampering.<br><br>**CVE ID: CVE-2025-22475** | https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities | O-DEL-DATA-170225/2315 |
| Affected Version(s): From (including) 7.13.1.0 Up to (excluding) 7.13.1.20 | | | | | |
| Insufficient Granularity of Access Control | 01-Feb-2025 | 7.8 | Dell PowerProtect DD versions prior to 8.3.0.0, 7.10.1.50, and 7.13.1.20 contain an improper access control vulnerability. A local malicious user with low privileges could potentially exploit this vulnerability leading to escalation of privilege.<br><br>**CVE ID: CVE-2024-53295** | https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities | O-DEL-DATA-170225/2316 |
| Affected Version(s): From (including) 7.14.0.0 Up to (excluding) 8.3.0.0 | | | | | |
| Insufficient Granularity of Access Control | 01-Feb-2025 | 7.8 | Dell PowerProtect DD versions prior to 8.3.0.0, 7.10.1.50, and 7.13.1.20 contain an improper access control vulnerability. A local malicious user with low privileges could potentially exploit this vulnerability leading to escalation of | https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple- | O-DEL-DATA-170225/2317 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege.<br>**CVE ID: CVE-2024-53295** | vulnerabilities | |
| Use of a Risky Cryptographic Primitive | 04-Feb-2025 | 3.7 | Dell PowerProtect DD, versions prior to DDOS 8.3.0.0, 7.10.1.50, and 7.13.1.10 contains a use of a Cryptographic Primitive with a Risky Implementation vulnerability. A remote attacker could potentially exploit this vulnerability, leading to Information tampering.<br>**CVE ID: CVE-2025-22475** | https://www.dell.com/support/kbdoc/en-us/000279157/dsa-2025-022-security-update-for-dell-powerprotect-dd-multiple-vulnerabilities | O-DEL-DATA-170225/2318 |
| **Vendor: Google** | | | | | |
| **Product: android** | | | | | |
| Affected Version(s): 12.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2319 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2320 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2321 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2322 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2323 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2324 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2325 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2326 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2327 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2066.<br>**CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2328 |
| Affected Version(s): 13.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2329 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2330 |
| Out-of-bounds | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a | https://corp.mediatek.com/pro | O-GOO-ANDR-170225/2331 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Write | | | missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | duct-security-bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2332 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2333 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2334 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2335 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2336 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066. | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2337 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20638** | | |
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2338 |
| Affected Version(s): 14.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2339 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2340 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This | https://corp.mediatek.com/product-security- | O-GOO-ANDR-170225/2341 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | bulletin/February-2025 | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2342 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2343 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2344 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2345 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2346 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2347 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Debug Messages Revealing Unnecessary Information | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br>**CVE ID: CVE-2025-20643** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2348 |
| Affected Version(s): 15.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.7 | In secmem, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS09403554; Issue ID: MSV-2431.<br>**CVE ID: CVE-2025-20636** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2349 |
| Write-what-where Condition | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291402; Issue ID: MSV-2073.<br>**CVE ID: CVE-2024-20141** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2350 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V5 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2351 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291406; Issue ID: MSV-2070.<br>**CVE ID: CVE-2024-20142** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2060.<br>**CVE ID: CVE-2025-20639** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2352 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2058.<br>**CVE ID: CVE-2025-20641** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2353 |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2354 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | MSV-2057.<br>**CVE ID: CVE-2025-20642** | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2355 |
| Use of Uninitialized Variable | 03-Feb-2025 | 4.3 | In DA, there is a possible read of uninitialized heap data due to uninitialized data. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291449; Issue ID: MSV-2066.<br>**CVE ID: CVE-2025-20638** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2356 |
| Out-of-bounds Read | 03-Feb-2025 | 4.3 | In DA, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2059.<br>**CVE ID: CVE-2025-20640** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-GOO-ANDR-170225/2357 |
| Debug Messages Revealing | 03-Feb-2025 | 3.9 | In DA, there is a possible out of bounds read due to a missing bounds check. This | https://corp.mediatek.com/product-security- | O-GOO-ANDR-170225/2358 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Unnecessary Information | | | could lead to local information disclosure, if an attacker has physical access to the device, if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS09291146; Issue ID: MSV-2056.<br><br>**CVE ID: CVE-2025-20643** | bulletin/February-2025 | |
| **Vendor: Linux** | | | | | |
| **Product: linux_kernel** | | | | | |
| Affected Version(s): * Up to (excluding) 5.4.290 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/45162febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2359 |
| Affected Version(s): 6.13 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2 | O-LIN-LINU-170225/2360 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear | b7ba6a256246ed82c365fdc686 | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>Revert "libfs: fix infinite directory reads for offset dir"<br><br>The current directory offset allocator (based on mtree_alloc_cyclic) stores the next offset value to return in octx->next_offset. This mechanism typically returns values that increase monotonically over time. Eventually, though, the newly allocated offset value wraps back to a low number (say, 2) which is smaller than other already-allocated offset values.<br><br>Yu Kuai <yukuai3@huawei.com> reports that, after commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir"), if a directory's offset allocator wraps, existing entries are no longer visible via readdir/getdents because offset_readdir() stops listing entries once an entry's offset is larger than octx->next_offset.<br>These entries vanish persistently -- they can be looked up, but will never again appear in readdir(3) output. | https://git.kernel.org/stable/c/3f250b82040a72b0059ae00855a74d8570ad2147, https://git.kernel.org/stable/c/9e9e710f68bac49bd9b587823c077d06363440e0, https://git.kernel.org/stable/c/b662d858131da9a8a14e68661656989b14dbf113 | O-LIN-LINU-170225/2361 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The reason for this is that the commit treats directory offsets as monotonically increasing integer values rather than opaque cookies, and introduces this comparison:<br><br>if (dentry2offset(dentry) >= last_index) {<br><br>On 64-bit platforms, the directory offset value upper bound is 2^63 - 1. Directory offsets will monotonically increase for millions of years without wrapping.<br><br>On 32-bit platforms, however, LONG_MAX is 2^31 - 1. The allocator can wrap after only a few weeks (at worst).<br><br>Revert commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir") to prepare for a fix that can work properly on 32-bit systems and might apply to recent LTS kernels where shmem employs the simple_offset mechanism.<br><br>**CVE ID: CVE-2024-57952** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after job completion<br><br>After a job completes, the corresponding pointer in | https://git.kernel.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8, https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a7 | O-LIN-LINU-170225/2362 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | the device must be set to NULL. Failing to do so triggers a warning when unloading the driver, as it appears the job is still active. To prevent this, assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | 67ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>mm: clear uffd-wp PTE/PMD state on mremap()<br><br>When mremap()ing a memory region previously registered with userfaultfd as write-protected but without UFFD_FEATURE_EVENT_REMAP, an inconsistency in flag clearing leads to a mismatch between the vma flags (which have uffd-wp cleared) and the pte/pmd flags (which do not have uffd-wp cleared). This mismatch causes a subsequent mprotect(PROT_WRITE) to trigger a warning in page_table_check_pte_flags() due to setting the pte to writable while uffd-wp is still set.<br><br>Fix this by always explicitly clearing the uffd-wp pte/pmd flags on any such mremap() so that the values are consistent with the existing clearing of VM_UFFD_WP. Be careful to clear the logical flag | https://git.kernel.org/stable/c/0cef0bb836e3cfe00f08f9606c72abd72fe78ca3, https://git.kernel.org/stable/c/310ac886d68de661c3a334198d8604b722d7fdf8 | O-LIN-LINU-170225/2363 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | regardless of its physical form; a PTE bit, a swap PTE bit, or a PTE marker. Cover PTE, huge PMD and hugetlb paths.<br><br>**CVE ID: CVE-2025-21696** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in __read_vmcore to (hopefully)<br>get rid of the softlockups. | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2364 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21694** | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gpio: xilinx: Convert gpio_lock to raw spinlock<br><br>irq_chip functions may be called in raw spinlock context. Therefore, we must also use a raw spinlock for our own internal locking.<br><br>This fixes the following lockdep splat:<br><br>[ 5.349336] ========== ========<br>[ 5.353349] [ BUG: Invalid wait context ]<br>[ 5.357361] 6.13.0-rc5+ #69 Tainted: G W<br>[ 5.363031] ---------- ----------<br>[ 5.367045] kworker/u17:1/44 is trying to lock:<br>[ 5.371587] ffffff88018b02c0 (&chip->gpio_lock){....}-{3:3}, at: xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8))<br>[ 5.380079] other info that might help us debug this:<br>[ 5.385138] context-{5:5}<br>[ 5.387762] 5 locks held by kworker/u17:1/44:<br>[ 5.392123] #0: ffffff8800014958 ((wq_completion)events_unbound){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3204)<br>[ 5.402260] #1: ffffffc082fcbdd8 | https://git.kernel.org/stable/c/9860370c2172704b6b4f0075a0c2a29fd84af96a, https://git.kernel.org/stable/c/9c035105c5537d2ecad6b9415e9417a1ffbd0a62, https://git.kernel.org/stable/c/b0111650ee596219bb5defa0ce1a1308e6e77ccf | O-LIN-LINU-170225/2365 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (deferred_probe_work){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3205) [ 5.411528] #2: ffffff880172c900 (&dev->mutex){....}-{4:4}, at: __device_attach (drivers/base/dd.c:1006) [ 5.419929] #3: ffffff88039c8268 (request_class#2){+.+.}-{4:4}, at: __setup_irq (kernel/irq/internals.h:156 kernel/irq/manage.c:1596) [ 5.428331] #4: ffffff88039c80c8 (lock_class#2){....}-{2:2}, at: __setup_irq (kernel/irq/manage.c:1614 ) [ 5.436472] stack backtrace: [ 5.439359] CPU: 2 UID: 0 PID: 44 Comm: kworker/u17:1 Tainted: G W 6.13.0-rc5+ #69 [ 5.448690] Tainted: [W]=WARN [ 5.451656] Hardware name: xlnx,zynqmp (DT) [ 5.455845] Workqueue: events_unbound deferred_probe_work_func [ 5.461699] Call trace: [ 5.464147] show_stack+0x18/0x24 C [ 5.467821] dump_stack_lvl (lib/dump_stack.c:123) [ 5.471501] dump_stack (lib/dump_stack.c:130) [ 5.474824] __lock_acquire (kernel/locking/lockdep.c:4828 kernel/locking/lockdep.c:4898 kernel/locking/lockdep.c:5176) [ 5.478758] lock_acquire (arch/arm64/include/asm/percpu.h: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 |
|---|---|---|---|---|---|
| | | | kernel/locking/lockdep.c:467 kernel/locking/lockdep.c:5851 kernel/locking/lockdep.c:5814) [ 5.482429] _raw_spin_lock_irqsave (include/linux/spinlock_api_smp.h:111 kernel/locking/spinlock.c:162) [ 5.486797] xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8)) [ 5.490737] irq_enable (kernel/irq/internals.h:236 kernel/irq/chip.c:170 kernel/irq/chip.c:439 kernel/irq/chip.c:432 kernel/irq/chip.c:345) [ 5.494060] __irq_startup (kernel/irq/internals.h:241 kernel/irq/chip.c:180 kernel/irq/chip.c:250) [ 5.497645] irq_startup (kernel/irq/chip.c:270) [ 5.501143] __setup_irq (kernel/irq/manage.c:1807) [ 5.504728] request_threaded_irq (kernel/irq/manage.c:2208)<br><br>**CVE ID: CVE-2025-21684** | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>irqchip/gic-v3-its: Don't enable interrupts in its_irq_set_vcpu_affinity()<br><br>The following call-chain leads to enabling interrupts in a nested interrupt disabled section: | https://git.kernel.org/stable/c/35cb2c6ce7da545f3b5cb1e6473ad7c3a6f08310, https://git.kernel.org/stable/c/6c84ff2e788fce0099ee3e71a3ed258b1ca1a223, https://git.kernel.org/stable/c/ | O-LIN-LINU-170225/2366 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | irq_set_vcpu_affinity()<br>irq_get_desc_lock()<br>raw_spin_lock_irqsave()<br><--- Disable interrupts<br>its_irq_set_vcpu_affinity()<br>guard(raw_spinlock_irq)<br><--- Enables interrupts when leaving the guard()<br>irq_put_desc_unlock()<br><--- Warns because interrupts are enabled<br><br>This was broken in commit b97e8a2f7130, which replaced the original raw_spin_[un]lock() pair with guard(raw_spinlock_irq).<br><br>Fix the issue by using guard(raw_spinlock).<br><br>[ tglx: Massaged change log ]<br>**CVE ID: CVE-2024-57949** | 93955a7788121ab5a0f7f27e988b2ed1135a4866 | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2367 |
| NULL Pointer Dereference | 12-Feb-2025 | 4.7 | In the Linux kernel, the following vulnerability has been resolved:<br><br>platform/x86: dell-uart-backlight: fix serdev race | https://git.kernel.org/stable/c/1b2128aa2d45ab20b22548dcf4b48906298ca7fd, | O-LIN-LINU-170225/2368 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The dell_uart_bl_serdev_probe() function calls devm_serdev_device_open() before setting the client ops via serdev_device_set_client_ops(). This ordering can trigger a NULL pointer dereference in the serdev controller's receive_buf handler, as it assumes serdev->ops is valid when SERPORT_ACTIVE is set.<br><br>This is similar to the issue fixed in commit 5e700b384ec1 ("platform/chrome: cros_ec_uart: properly fix race condition") where devm_serdev_device_open() was called before fully initializing the device.<br><br>Fix the race by ensuring client ops are set before enabling the port via devm_serdev_device_open().<br><br>Note, serdev_device_set_baudrate() and serdev_device_set_flow_control() calls should be after the devm_serdev_device_open() call.<br><br>**CVE ID: CVE-2025-21695** | https://git.kernel.org/stable/c/d3a24d923333f75aaece9acb051d676edc0afb75 | |
| NULL Pointer Dereference | 09-Feb-2025 | 4.7 | In the Linux kernel, the following vulnerability has been resolved:<br><br>platform/x86: lenovo-yoga-tab2-pro-1380-fastcharger: fix serdev race | https://git.kernel.org/stable/c/3f67e07873df3c6d9ce2582260b83732e1d3a40b, https://git.kern | O-LIN-LINU-170225/2369 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | The yt2_1380_fc_serdev_probe() function calls devm_serdev_device_open() before setting the client ops via serdev_device_set_client_ops(). This ordering can trigger a NULL pointer dereference in the serdev controller's receive_buf handler, as it assumes serdev->ops is valid when SERPORT_ACTIVE is set.<br><br>This is similar to the issue fixed in commit 5e700b384ec1 ("platform/chrome: cros_ec_uart: properly fix race condition") where devm_serdev_device_open() was called before fully initializing the device.<br><br>Fix the race by ensuring client ops are set before enabling the port via devm_serdev_device_open().<br><br>Note, serdev_device_set_baudrate() and serdev_device_set_flow_control() calls should be after the devm_serdev_device_open() call.<br><br>**CVE ID: CVE-2025-21685** | el.org/stable/c/59616a91e5e74833b2008b56c66879857c616006 | |
| Affected Version(s): From (including) 4.19 Up to (excluding) 5.4.290 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after | https://git.kernel.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8, | O-LIN-LINU-170225/2370 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | |
| Affected Version(s): From (including) 4.19.302 Up to (excluding) 4.20 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | O-LIN-LINU-170225/2371 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 4.19.317 Up to (excluding) 4.20 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836 | O-LIN-LINU-170225/2372 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in __read_vmcore to (hopefully)<br>get rid of the softlockups.<br><br>**CVE ID: CVE-2025-21694** | ,<br>https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | |
| Affected Version(s): From (including) 5.10.204 Up to (excluding) 5.10.234 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7,<br>https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a,<br>https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | O-LIN-LINU-170225/2373 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1 after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | prepare callback ]<br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 5.10.221 Up to (excluding) 5.10.234 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in __read_vmcore to (hopefully)<br>get rid of the softlockups.<br>**CVE ID: CVE-2025-21694** | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a,<br>https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836,<br>https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2374 |
| Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.177 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the | https://git.kern | O-LIN-LINU- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | el.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8, https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | 170225/2375 |
| Affected Version(s): From (including) 5.11 Up to (excluding) 5.15.178 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2376 |
| Affected Version(s): From (including) 5.12 Up to (excluding) 6.6.74 | | | | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gpio: xilinx: Convert gpio_lock to raw spinlock | https://git.kernel.org/stable/c/9860370c2172704b6b4f0075a0c2a29fd84af96a, https://git.kernel.org/stable/c/ | O-LIN-LINU-170225/2377 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | irq_chip functions may be called in raw spinlock context. Therefore, we must also use a raw spinlock for our own internal locking.<br><br>This fixes the following lockdep splat:<br><br>[ 5.349336] ========== ========<br>[ 5.353349] [ BUG: Invalid wait context ]<br>[ 5.357361] 6.13.0-rc5+ #69 Tainted: G W<br>[ 5.363031] ---------- ----------<br>[ 5.367045] kworker/u17:1/44 is trying to lock:<br>[ 5.371587] ffffff88018b02c0 (&chip->gpio_lock){....}-{3:3}, at: xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8))<br>[ 5.380079] other info that might help us debug this:<br>[ 5.385138] context-{5:5}<br>[ 5.387762] 5 locks held by kworker/u17:1/44:<br>[ 5.392123] #0: ffffff8800014958 ((wq_completion)events_unbound){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3204)<br>[ 5.402260] #1: ffffffc082fcbdd8 (deferred_probe_work){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3205)<br>[ 5.411528] #2: ffffff880172c900 (&dev->mutex){....}-{4:4}, at: __device_attach (drivers/base/dd.c:1006)<br>[ 5.419929] #3: | 9c035105c5537d2ecad6b9415e9417a1ffbd0a62, https://git.kernel.org/stable/c/b0111650ee596219bb5defa0ce1a1308e6e77ccf | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ffffff88039c8268 (request_class#2){+.+.}-{4:4}, at: __setup_irq (kernel/irq/internals.h:156 kernel/irq/manage.c:1596) [ 5.428331] #4: ffffff88039c80c8 (lock_class#2){....}-{2:2}, at: __setup_irq (kernel/irq/manage.c:1614 ) [ 5.436472] stack backtrace: [ 5.439359] CPU: 2 UID: 0 PID: 44 Comm: kworker/u17:1 Tainted: G W 6.13.0-rc5+ #69 [ 5.448690] Tainted: [W]=WARN [ 5.451656] Hardware name: xlnx,zynqmp (DT) [ 5.455845] Workqueue: events_unbound deferred_probe_work_func [ 5.461699] Call trace: [ 5.464147] show_stack+0x18/0x24 C [ 5.467821] dump_stack_lvl (lib/dump_stack.c:123) [ 5.471501] dump_stack (lib/dump_stack.c:130) [ 5.474824] __lock_acquire (kernel/locking/lockdep.c:4828 kernel/locking/lockdep.c:4898 kernel/locking/lockdep.c:5176) [ 5.478758] lock_acquire (arch/arm64/include/asm/percpu.h:40 kernel/locking/lockdep.c:467 kernel/locking/lockdep.c:5851 kernel/locking/lockdep.c:5814) [ 5.482429] _raw_spin_lock_irqsave (include/linux/spinlock_api_smp.h:111 | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | kernel/locking/spinlock.c:162)<br>[ 5.486797] xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8))<br>[ 5.490737] irq_enable (kernel/irq/internals.h:236 kernel/irq/chip.c:170 kernel/irq/chip.c:439 kernel/irq/chip.c:432 kernel/irq/chip.c:345)<br>[ 5.494060] __irq_startup (kernel/irq/internals.h:241 kernel/irq/chip.c:180 kernel/irq/chip.c:250)<br>[ 5.497645] irq_startup (kernel/irq/chip.c:270)<br>[ 5.501143] __setup_irq (kernel/irq/manage.c:1807)<br>[ 5.504728] request_threaded_irq (kernel/irq/manage.c:2208)<br><br>**CVE ID: CVE-2025-21684** | | |
| Affected Version(s): From (including) 5.15.143 Up to (excluding) 5.15.177 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | O-LIN-LINU-170225/2378 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 5.15.162 Up to (excluding) 5.15.177 | | | | | |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in __read_vmcore to (hopefully)<br>get rid of the softlockups.<br><br>**CVE ID: CVE-2025-21694** | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2379 |
| Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.127 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after | https://git.kernel.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8, | O-LIN-LINU-170225/2380 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | |
| Affected Version(s): From (including) 5.16 Up to (excluding) 6.1.128 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2381 |
| Affected Version(s): From (including) 5.4.264 Up to (excluding) 5.4.290 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kern | O-LIN-LINU-170225/2382 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online | el.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 5.4.279 Up to (excluding) 5.4.290 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in __read_vmcore to (hopefully)<br>get rid of the softlockups. | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2383 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21694** | | |
| Affected Version(s): From (including) 5.5 Up to (excluding) 5.10.234 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | https://git.kernel.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8, https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | O-LIN-LINU-170225/2384 |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2385 |
| Affected Version(s): From (including) 5.7 Up to (excluding) 6.12.11 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved: | https://git.kernel.org/stable/c/0cef0bb836e3cfe00f08f9606c72 | O-LIN-LINU-170225/2386 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | mm: clear uffd-wp PTE/PMD state on mremap()<br><br>When mremap()ing a memory region previously registered with userfaultfd as write-protected but without UFFD_FEATURE_EVENT_REMAP, an inconsistency in flag clearing leads to a mismatch between the vma flags (which have uffd-wp cleared) and the pte/pmd flags (which do not have uffd-wp cleared). This mismatch causes a subsequent mprotect(PROT_WRITE) to trigger a warning in page_table_check_pte_flags() due to setting the pte to writable while uffd-wp is still set.<br><br>Fix this by always explicitly clearing the uffd-wp pte/pmd flags on any such mremap() so that the values are consistent with the existing clearing of VM_UFFD_WP. Be careful to clear the logical flag regardless of its physical form; a PTE bit, a swap PTE bit, or a PTE marker. Cover PTE, huge PMD and hugetlb paths.<br><br>**CVE ID: CVE-2025-21696** | abd72fe78ca3, https://git.kernel.org/stable/c/310ac886d68de661c3a334198d8604b722d7fdf8 | |
| Affected Version(s): From (including) 6.1.68 Up to (excluding) 6.1.127 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/ | O-LIN-LINU-170225/2387 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1 after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag. | 15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | [ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 6.1.95 Up to (excluding) 6.1.127 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2388 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | second loop in __read_vmcore to (hopefully) get rid of the softlockups.<br><br>**CVE ID: CVE-2025-21694** | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>irqchip/gic-v3-its: Don't enable interrupts in its_irq_set_vcpu_affinity()<br><br>The following call-chain leads to enabling interrupts in a nested interrupt disabled section:<br><br>irq_set_vcpu_affinity()<br>irq_get_desc_lock()<br>raw_spin_lock_irqsave()<br><--- Disable interrupts<br>its_irq_set_vcpu_affinity()<br>guard(raw_spinlock_irq)<br><--- Enables interrupts when leaving the guard()<br>irq_put_desc_unlock()<br><--- Warns because interrupts are enabled<br><br>This was broken in commit b97e8a2f7130, which replaced the original raw_spin_[un]lock() pair with guard(raw_spinlock_irq).<br><br>Fix the issue by using guard(raw_spinlock).<br><br>[ tglx: Massaged change log ]<br><br>**CVE ID: CVE-2024-57949** | https://git.kernel.org/stable/c/35cb2c6ce7da545f3b5cb1e6473ad7c3a6f08310, https://git.kernel.org/stable/c/6c84ff2e788fce0099ee3e71a3ed258b1ca1a223, https://git.kernel.org/stable/c/93955a7788121ab5a0f7f27e988b2ed1135a4866 | O-LIN-LINU-170225/2389 |
| Affected Version(s): From (including) 6.10 Up to (excluding) 6.12.11 | | | | | |
| NULL Pointer Dereference | 09-Feb-2025 | 4.7 | In the Linux kernel, the following vulnerability has been resolved:<br><br>platform/x86: lenovo-yoga- | https://git.kernel.org/stable/c/3f67e07873df3c6d9ce2582260b83732e1d3a40b | O-LIN-LINU-170225/2390 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | tab2-pro-1380-fastcharger: fix serdev race<br><br>The yt2_1380_fc_serdev_probe() function calls devm_serdev_device_open() before setting the client ops via serdev_device_set_client_ops(). This ordering can trigger a NULL pointer dereference in the serdev controller's receive_buf handler, as it assumes serdev->ops is valid when SERPORT_ACTIVE is set.<br><br>This is similar to the issue fixed in commit 5e700b384ec1 ("platform/chrome: cros_ec_uart: properly fix race condition") where devm_serdev_device_open() was called before fully initializing the device.<br><br>Fix the race by ensuring client ops are set before enabling the port via devm_serdev_device_open().<br><br>Note, serdev_device_set_baudrate() and serdev_device_set_flow_control() calls should be after the devm_serdev_device_open() call.<br><br>**CVE ID: CVE-2025-21685** | ,<br>https://git.kernel.org/stable/c/59616a91e5e74833b2008b56c66879857c616006 | |
| NULL Pointer Dereference | 12-Feb-2025 | 4.7 | In the Linux kernel, the following vulnerability has been resolved:<br><br>platform/x86: dell-uart- | https://git.kernel.org/stable/c/1b2128aa2d45ab20b22548dcf4b48906298ca7f | O-LIN-LINU-170225/2391 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | backlight: fix serdev race<br><br>The dell_uart_bl_serdev_probe() function calls devm_serdev_device_open() before setting the client ops via serdev_device_set_client_ops(). This ordering can trigger a NULL pointer dereference in the serdev controller's receive_buf handler, as it assumes serdev->ops is valid when SERPORT_ACTIVE is set.<br><br>This is similar to the issue fixed in commit 5e700b384ec1 ("platform/chrome: cros_ec_uart: properly fix race condition") where devm_serdev_device_open() was called before fully initializing the device.<br><br>Fix the race by ensuring client ops are set before enabling the port via devm_serdev_device_open().<br><br>Note, serdev_device_set_baudrate() and serdev_device_set_flow_control() calls should be after the devm_serdev_device_open() call.<br><br>**CVE ID: CVE-2025-21695** | d, https://git.kernel.org/stable/c/d3a24d923333f75aaece9acb051d676edc0afb75 | |
| Affected Version(s): From (including) 6.11 Up to (excluding) 6.12.12 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>Revert "libfs: fix infinite | https://git.kernel.org/stable/c/3f250b82040a72b0059ae00855a74d8570ad214 | O-LIN-LINU-170225/2392 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | directory reads for offset dir"<br><br>The current directory offset allocator (based on mtree_alloc_cyclic) stores the next offset value to return in octx->next_offset. This mechanism typically returns values that increase monotonically over time. Eventually, though, the newly allocated offset value wraps back to a low number (say, 2) which is smaller than other already-allocated offset values.<br><br>Yu Kuai <yukuai3@huawei.com> reports that, after commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir"), if a directory's offset allocator wraps, existing entries are no longer visible via readdir/getdents because offset_readdir() stops listing entries once an entry's offset is larger than octx->next_offset.<br>These entries vanish persistently -- they can be looked up, but will never again appear in readdir(3) output.<br><br>The reason for this is that the commit treats directory offsets as monotonically increasing integer values rather than opaque cookies, and introduces this comparison:<br><br>if (dentry2offset(dentry) >= | 7, https://git.kernel.org/stable/c/9e9e710f68bac49bd9b587823c077d06363440e0, https://git.kernel.org/stable/c/b662d858131da9a8a14e68661656989b14dbf113 | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | last_index) {<br><br>On 64-bit platforms, the directory offset value upper bound is 2^63 - 1. Directory offsets will monotonically increase for millions of years without wrapping.<br><br>On 32-bit platforms, however, LONG_MAX is 2^31 - 1. The allocator can wrap after only a few weeks (at worst).<br><br>Revert commit 64a7ce76fb90 ("libfs: fix infinite directory reads for offset dir") to prepare for a fix that can work properly on 32-bit systems and might apply to recent LTS kernels where shmem employs the simple_offset mechanism.<br><br>**CVE ID: CVE-2024-57952** | | |
| Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.74 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating<br>the job has finished. | https://git.kernel.org/stable/c/14e0a874488e79086340ba8e2d238cb9596b68a8,<br>https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd,<br>https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | O-LIN-LINU-170225/2393 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21697** | | |
| Affected Version(s): From (including) 6.2 Up to (excluding) 6.6.75 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2394 |
| Affected Version(s): From (including) 6.6.35 Up to (excluding) 6.6.74 | | | | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>irqchip/gic-v3-its: Don't enable interrupts in its_irq_set_vcpu_affinity()<br><br>The following call-chain leads to enabling interrupts in a nested interrupt disabled section:<br><br>irq_set_vcpu_affinity()<br>irq_get_desc_lock()<br>raw_spin_lock_irqsave()<br><--- Disable interrupts<br>its_irq_set_vcpu_affinity()<br>guard(raw_spinlock_irq)<br><--- Enables interrupts when leaving the guard()<br>irq_put_desc_unlock()<br><--- Warns because interrupts are enabled<br><br>This was broken in commit b97e8a2f7130, which | https://git.kernel.org/stable/c/35cb2c6ce7da545f3b5cb1e6473ad7c3a6f08310, https://git.kernel.org/stable/c/6c84ff2e788fce0099ee3e71a3ed258b1ca1a223, https://git.kernel.org/stable/c/93955a7788121ab5a0f7f27e988b2ed1135a4866 | O-LIN-LINU-170225/2395 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | replaced the original raw_spin_[un]lock() pair with guard(raw_spinlock_irq).<br><br>Fix the issue by using guard(raw_spinlock).<br><br>[ tglx: Massaged change log ]<br><br>**CVE ID: CVE-2024-57949** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is<br>not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural<br>sleep points, like scheduling out while waiting for a data write to<br>happen, but apparently that is not always enough.<br><br>Add a cond_resched() to the second loop in | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2396 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | __read_vmcore to (hopefully) get rid of the softlockups.<br>**CVE ID: CVE-2025-21694** | | |
| Affected Version(s): From (including) 6.6.7 Up to (excluding) 6.6.74 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | O-LIN-LINU-170225/2397 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.11 | | | | | |
| Use After Free | 12-Feb-2025 | 7.8 | In the Linux kernel, the following vulnerability has been resolved:<br><br>hrtimers: Handle CPU state correctly on hotplug<br><br>Consider a scenario where a CPU transitions from CPUHP_ONLINE to halfway through a CPU hotunplug down to CPUHP_HRTIMERS_PREPARE, and then back to CPUHP_ONLINE:<br><br>Since hrtimers_prepare_cpu() does not run, cpu_base.hres_active remains set to 1 throughout. However, during a CPU unplug | https://git.kernel.org/stable/c/14984139f1f2768883332965db566ef26db609e7, https://git.kernel.org/stable/c/15b453db41d36184cf0ccc21e7df624014ab6a1a, https://git.kernel.org/stable/c/2f8dea1692eef2b7ba6a256246ed82c365fdc686 | O-LIN-LINU-170225/2398 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | operation, the tick and the clockevents are shut down at CPUHP_AP_TICK_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP_HRTIMERS_PREPARE once.<br><br>This round-trip reveals another issue; cpu_base.online is not set to 1<br>after the transition, which appears as a WARN_ON_ONCE in enqueue_hrtimer().<br><br>Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.<br><br>Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.<br><br>[ tglx: Make the new callback unconditionally available, remove the online modification in the prepare() callback and clear the remaining state in the starting callback instead of the prepare callback ]<br><br>**CVE ID: CVE-2024-57951** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has | https://git.kernel.org/stable/c/ | O-LIN-LINU-170225/2399 |

| 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 |
|---|---|---|---|---|---|
| | | | been resolved:<br><br>drm/v3d: Ensure job pointer is set to NULL after job completion<br><br>After a job completes, the corresponding pointer in the device must be set to NULL. Failing to do so triggers a warning when unloading<br>the driver, as it appears the job is still active. To prevent this,<br>assign the job pointer to NULL after completing the job, indicating the job has finished.<br><br>**CVE ID: CVE-2025-21697** | 14e0a874488e79086340ba8e2d238cb9596b68a8, https://git.kernel.org/stable/c/1bd6303d08c85072ce40ac01a767ab67195105bd, https://git.kernel.org/stable/c/2a1c88f7ca5c12dff6fa6787492ac910bb9e4407 | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gpio: xilinx: Convert gpio_lock to raw spinlock<br><br>irq_chip functions may be called in raw spinlock context. Therefore, we must also use a raw spinlock for our own internal locking.<br><br>This fixes the following lockdep splat:<br><br>[ 5.349336] ========== ========<br>[ 5.353349] [ BUG: Invalid wait context ]<br>[ 5.357361] 6.13.0-rc5+ #69 Tainted: G W<br>[ 5.363031] ---------- ----------<br>[ 5.367045] kworker/u17:1/44 is trying to lock:<br>[ 5.371587] | https://git.kernel.org/stable/c/9860370c2172704b6b4f0075a0c2a29fd84af96a, https://git.kernel.org/stable/c/9c035105c5537d2ecad6b9415e9417a1ffbd0a62, https://git.kernel.org/stable/c/b0111650ee596219bb5defa0ce1a1308e6e77ccf | O-LIN-LINU-170225/2400 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | ffffff88018b02c0 (&chip->gpio_lock){....}-{3:3}, at: xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8))<br>[ 5.380079] other info that might help us debug this:<br>[ 5.385138] context-{5:5}<br>[ 5.387762] 5 locks held by kworker/u17:1/44:<br>[ 5.392123] #0: ffffff8800014958 ((wq_completion)events_unbound){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3204)<br>[ 5.402260] #1: ffffffc082fcbdd8 (deferred_probe_work){+.+.}-{0:0}, at: process_one_work (kernel/workqueue.c:3205)<br>[ 5.411528] #2: ffffff880172c900 (&dev->mutex){....}-{4:4}, at: __device_attach (drivers/base/dd.c:1006)<br>[ 5.419929] #3: ffffff88039c8268 (request_class#2){+.+.}-{4:4}, at: __setup_irq (kernel/irq/internals.h:156 kernel/irq/manage.c:1596)<br>[ 5.428331] #4: ffffff88039c80c8 (lock_class#2){....}-{2:2}, at: __setup_irq (kernel/irq/manage.c:1614)<br>[ 5.436472] stack backtrace:<br>[ 5.439359] CPU: 2 UID: 0 PID: 44 Comm: kworker/u17:1 Tainted: G W 6.13.0-rc5+ #69<br>[ 5.448690] Tainted: [W]=WARN<br>[ 5.451656] Hardware name: xlnx,zynqmp (DT)<br>[ 5.455845] Workqueue: events_unbound | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | deferred_probe_work_func [ 5.461699] Call trace: [ 5.464147] show_stack+0x18/0x24 C [ 5.467821] dump_stack_lvl (lib/dump_stack.c:123) [ 5.471501] dump_stack (lib/dump_stack.c:130) [ 5.474824] __lock_acquire (kernel/locking/lockdep.c:4828 kernel/locking/lockdep.c:4898 kernel/locking/lockdep.c:5176) [ 5.478758] lock_acquire (arch/arm64/include/asm/percpu.h:40 kernel/locking/lockdep.c:467 kernel/locking/lockdep.c:5851 kernel/locking/lockdep.c:5814) [ 5.482429] _raw_spin_lock_irqsave (include/linux/spinlock_api_smp.h:111 kernel/locking/spinlock.c:162) [ 5.486797] xgpio_irq_unmask (drivers/gpio/gpio-xilinx.c:433 (discriminator 8)) [ 5.490737] irq_enable (kernel/irq/internals.h:236 kernel/irq/chip.c:170 kernel/irq/chip.c:439 kernel/irq/chip.c:432 kernel/irq/chip.c:345) [ 5.494060] __irq_startup (kernel/irq/internals.h:241 kernel/irq/chip.c:180 kernel/irq/chip.c:250) [ 5.497645] irq_startup (kernel/irq/chip.c:270) [ 5.501143] __setup_irq (kernel/irq/manage.c:1807 ) [ 5.504728] | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | request_threaded_irq (kernel/irq/manage.c:2208 )<br><br>**CVE ID: CVE-2025-21684** | | |
| Affected Version(s): From (including) 6.7 Up to (excluding) 6.12.12 | | | | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>gfs2: Truncate address space when flipping GFS2_DIF_JDATA flag<br><br>Truncate an inode's address space when flipping the GFS2_DIF_JDATA flag: depending on that flag, the pages in the address space will either use buffer heads or iomap_folio_state structs, and we cannot mix the two.<br><br>**CVE ID: CVE-2025-21699** | https://git.kernel.org/stable/c/2a40a140e11fec699e128170ccaa98b6b82cb503, https://git.kernel.org/stable/c/2b0bd5051ad1c1e9ef4879f18e15a7712c974f3e, https://git.kernel.org/stable/c/4516febe325342555bb09ca5b396fb816d655821 | O-LIN-LINU-170225/2401 |
| Affected Version(s): From (including) 6.9.6 Up to (excluding) 6.12.11 | | | | | |
| Improper Locking | 09-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>irqchip/gic-v3-its: Don't enable interrupts in its_irq_set_vcpu_affinity()<br><br>The following call-chain leads to enabling interrupts in a nested interrupt disabled section:<br><br>irq_set_vcpu_affinity()<br>irq_get_desc_lock()<br>raw_spin_lock_irqsave()<br><--- Disable interrupts<br>its_irq_set_vcpu_affinity()<br>guard(raw_spinlock_irq)<br><--- Enables interrupts when leaving the guard()<br>irq_put_desc_unlock()<br><--- Warns because interrupts are enabled | https://git.kernel.org/stable/c/35cb2c6ce7da545f3b5cb1e6473ad7c3a6f08310, https://git.kernel.org/stable/c/6c84ff2e788fce0099ee3e71a3ed258b1ca1a223, https://git.kernel.org/stable/c/93955a7788121ab5a0f7f27e988b2ed1135a4866 | O-LIN-LINU-170225/2402 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | This was broken in commit b97e8a2f7130, which replaced the original raw_spin_[un]lock() pair with guard(raw_spinlock_irq).<br><br>Fix the issue by using guard(raw_spinlock).<br><br>[ tglx: Massaged change log ]<br><br>**CVE ID: CVE-2024-57949** | | |
| N/A | 12-Feb-2025 | 5.5 | In the Linux kernel, the following vulnerability has been resolved:<br><br>fs/proc: fix softlockup in __read_vmcore (part 2)<br><br>Since commit 5cbcb62dddf5 ("fs/proc: fix softlockup in __read_vmcore") the number of softlockups in __read_vmcore at kdump time have gone down, but they still happen sometimes.<br><br>In a memory constrained environment like the kdump image, a softlockup is not just a harmless message, but it can interfere with things like RCU freeing memory, causing the crashdump to get stuck.<br><br>The second loop in __read_vmcore has a lot more opportunities for natural sleep points, like scheduling out while waiting for a data write to happen, but apparently that is not always enough. | https://git.kernel.org/stable/c/649b266606bc413407ce315f710c8ce8a88ee30a, https://git.kernel.org/stable/c/65c367bd9d4f43513c7f837df5753bea9561b836, https://git.kernel.org/stable/c/80828540dad0757b6337c6561d49c81038f38d87 | O-LIN-LINU-170225/2403 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Add a cond_resched() to the second loop in __read_vmcore to (hopefully) get rid of the softlockups.<br>**CVE ID: CVE-2025-21694** | | |
| **Vendor: mediatek** | | | | | |
| **Product: nr16** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-MED-NR16-170225/2404 |
| **Product: nr17** | | | | | |
| Affected Version(s): - | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-MED-NR17-170225/2405 |
| **Product: nr17r** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 03-Feb-2025 | 9.8 | In Modem, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution, if a UE has connected to a rogue base station controlled by the attacker, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01289384; Issue ID: MSV-2436.<br>**CVE ID: CVE-2025-20634** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-MED-NR17-170225/2406 |
| **Vendor: Microsoft** | | | | | |
| **Product: windows_10_1507** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.10240.20915 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2407 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2408 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2409 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2410 |
| Improper Link Resolution Before File Access | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | O-MIC-WIND-170225/2411 |

| 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 |
|---|---|---|---|---|---|
| ('Link Following') | | | | 21391 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability<br>**CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2412 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2413 |
| **Product: windows_10_1607** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.10240.20915 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2414 |
| Affected Version(s): * Up to (excluding) 10.0.14393.7785 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2415 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2416 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2417 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2418 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2419 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability<br>**CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2420 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2421 |
| **Product: windows_10_1809** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.17763.6893 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2422 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2423 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2424 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2425 |
| Improper Link Resolution Before File | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability | https://msrc.microsoft.com/update-guide/vulnerabi | O-MIC-WIND-170225/2426 |

| 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 |
|---|---|---|---|---|---|
| Access ('Link Following') | | | **CVE ID: CVE-2025-21419** | lity/CVE-2025-21419 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2427 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2428 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2429 |
| **Product: windows_10_21h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.19044.5487 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2430 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2431 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2432 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2433 |
| Improper | 11-Feb-2025 | 7.1 | Windows Setup Files | https://msrc.mi | O-MIC-WIND- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Link Resolution Before File Access ('Link Following') | | | Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | crosoft.com/update-guide/vulnerability/CVE-2025-21419 | 170225/2434 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2435 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2436 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2437 |
| **Product: windows_10_22h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.19045.5487 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2438 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2439 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2440 |
| Improper Link Resolution Before File Access | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | O-MIC-WIND-170225/2441 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| ('Link Following') | | | | 21420 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2442 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2443 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2444 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2445 |
| **Product: windows_11_22h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.22621.4890 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2446 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2447 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2448 |
| Improper Link | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege | https://msrc.microsoft.com/upd | O-MIC-WIND-170225/2449 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | Vulnerability<br>**CVE ID: CVE-2025-21420** | ate-guide/vulnerability/CVE-2025-21420 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2450 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2451 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability<br>**CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2452 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2453 |
| **Product: windows_11_23h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.22631.4890 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2454 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2455 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | O-MIC-WIND-170225/2456 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21418** | 21418 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2457 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2458 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2459 |
| Affected Version(s): * Up to (including) 10.0.22631.4890 | | | | | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2460 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2461 |
| **Product: windows_11_24h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.26100.3194 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2462 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- | O-MIC-WIND-170225/2463 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | 21406 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2464 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2465 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2466 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2467 |
| Use After Free | 11-Feb-2025 | 7.1 | DHCP Client Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21379** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21379 | O-MIC-WIND-170225/2468 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability<br>**CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2469 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2470 |
| **Product: windows_server_2008** | | | | | |
| Affected Version(s): - | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code | https://msrc.microsoft.com/upd | O-MIC-WIND-170225/2471 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | ate-guide/vulnerability/CVE-2025-21406 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2472 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2473 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2474 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2475 |
| Affected Version(s): r2 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2476 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2477 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2478 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of | https://msrc.microsoft.com/update- | O-MIC-WIND-170225/2479 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | guide/vulnerability/CVE-2025-21418 | |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2480 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2481 |
| **Product: windows_server_2012** | | | | | |
| Affected Version(s): - | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2482 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2483 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2484 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2485 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2486 |
| Improper | 11-Feb-2025 | 7.1 | Windows Setup Files | https://msrc.mi | O-MIC-WIND- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Link Resolution Before File Access ('Link Following') | | | Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | crosoft.com/update-guide/vulnerability/CVE-2025-21419 | 170225/2487 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2488 |
| Affected Version(s): r2 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2489 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2490 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2491 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2492 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2493 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2494 |

| 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 |
|---|---|---|---|---|---|
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2495 |
| **Product: windows_server_2016** | | | | | |
| Affected Version(s): - | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2496 |
| Affected Version(s): * Up to (excluding) 10.0.14393.7785 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2497 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2498 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability<br>**CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2499 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2500 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability<br>**CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2501 |
| Improper Link | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability | https://msrc.microsoft.com/upd | O-MIC-WIND-170225/2502 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Resolution Before File Access ('Link Following') | | | **CVE ID: CVE-2025-21391** | ate-guide/vulnerability/CVE-2025-21391 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2503 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2504 |
| **Product: windows_server_2019** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.17763.6893 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2505 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2506 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2507 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2508 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2509 |

| 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 |
|---|---|---|---|---|---|
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2510 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2511 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2512 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2513 |
| **Product: windows_server_2022** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.20348.3207 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2514 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2515 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2516 |
| Improper Link Resolution Before File | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability | https://msrc.microsoft.com/update-guide/vulnerabi | O-MIC-WIND-170225/2517 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Access ('Link Following') | | | **CVE ID: CVE-2025-21420** | lity/CVE-2025-21420 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2518 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2519 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2520 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2521 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2522 |
| **Product: windows_server_2022_23h2** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.25398.1425 | | | | | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2523 |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21406** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21406 | O-MIC-WIND-170225/2524 |
| Heap-based | 11-Feb-2025 | 8.8 | Windows Telephony | https://msrc.mi | O-MIC-WIND- |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | crosoft.com/update-guide/vulnerability/CVE-2025-21407 | 170225/2525 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2526 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2527 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2528 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2529 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability **CVE ID: CVE-2025-21414** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21414 | O-MIC-WIND-170225/2530 |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability **CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2531 |
| **Product: windows_server_2025** | | | | | |
| Affected Version(s): * Up to (excluding) 10.0.26100.3194 | | | | | |
| Use After Free | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability | https://msrc.microsoft.com/update-guide/vulnerabi | O-MIC-WIND-170225/2532 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21406** | lity/CVE-2025-21406 | |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability **CVE ID: CVE-2025-21410** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21410 | O-MIC-WIND-170225/2533 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 8.8 | Windows Telephony Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21407** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21407 | O-MIC-WIND-170225/2534 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7.8 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21418** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21418 | O-MIC-WIND-170225/2535 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.8 | Windows Disk Cleanup Tool Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21420** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420 | O-MIC-WIND-170225/2536 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Setup Files Cleanup Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21419** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21419 | O-MIC-WIND-170225/2537 |
| Use After Free | 11-Feb-2025 | 7.1 | DHCP Client Service Remote Code Execution Vulnerability **CVE ID: CVE-2025-21379** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21379 | O-MIC-WIND-170225/2538 |
| Improper Link Resolution Before File Access ('Link Following') | 11-Feb-2025 | 7.1 | Windows Storage Elevation of Privilege Vulnerability **CVE ID: CVE-2025-21391** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21391 | O-MIC-WIND-170225/2539 |
| Heap-based Buffer Overflow | 11-Feb-2025 | 7 | Windows Core Messaging Elevation of Privileges Vulnerability | https://msrc.microsoft.com/update-guide/vulnerabi | O-MIC-WIND-170225/2540 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-21414** | lity/CVE-2025-21414 | |
| External Control of File Name or Path | 11-Feb-2025 | 6.5 | NTLM Hash Disclosure Spoofing Vulnerability<br>**CVE ID: CVE-2025-21377** | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21377 | O-MIC-WIND-170225/2541 |
| **Vendor: openatom** | | | | | |
| **Product: openharmony** | | | | | |
| Affected Version(s): From (including) 4.1.0 Up to (including) 4.1.2 | | | | | |
| Use After Free | 07-Feb-2025 | 8.8 | in OpenHarmony v4.1.2 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through use after free.<br>**CVE ID: CVE-2025-0304** | https://gitee.com/openharmony/security/blob/master/zh/security-disclosure/2025/2025-02.md | O-OPE-OPEN-170225/2542 |
| Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') | 07-Feb-2025 | 8.8 | in OpenHarmony v4.1.2 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through buffer overflow.<br>**CVE ID: CVE-2025-0303** | N/A | O-OPE-OPEN-170225/2543 |
| Integer Overflow or Wraparound | 07-Feb-2025 | 5.5 | in OpenHarmony v4.1.2 and prior versions allow a local attacker cause DOS through integer overflow.<br>**CVE ID: CVE-2025-0302** | N/A | O-OPE-OPEN-170225/2544 |
| **Vendor: openwrt** | | | | | |
| **Product: openwrt** | | | | | |
| Affected Version(s): 19.07.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-OPE-OPEN-170225/2545 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | | |
| Affected Version(s): 21.02.0 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-OPE-OPEN-170225/2546 |
| Affected Version(s): 22.03.5 | | | | | |
| Out-of-bounds Write | 03-Feb-2025 | 6.6 | In V6 DA, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege, if an attacker has physical access to the device, with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09403752; Issue ID: MSV-2434.<br>**CVE ID: CVE-2025-20635** | https://corp.mediatek.com/product-security-bulletin/February-2025 | O-OPE-OPEN-170225/2547 |
| **Vendor: Qualcomm** | | | | | |
| **Product: aqt1000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AQT1-170225/2548 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AQT1-170225/2549 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AQT1-170225/2550 |
| **Product: ar8035_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2551 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2552 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2553 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2554 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-AR80-170225/2555 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2556 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2557 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2558 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-AR80-170225/2559 |
| **Product: c-v2x_9150_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-C-V2-170225/2560 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-C-V2-170225/2561 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-C-V2-170225/2562 |

| 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 |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| **Product: csr8811_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-CSR8-170225/2563 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-CSR8-170225/2564 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-CSR8-170225/2565 |
| **Product: csra6620_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-CSRA-170225/2566 |
| **Product: csra6640_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-CSRA-170225/2567 |
| **Product: csrb31024_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-CSRB- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| check Time-of-use (TOCTOU) Race Condition | | | parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2568 |
| **Product: fastconnect_6200_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2569 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2570 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2571 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2572 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2573 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2574 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2575 |
| **Product: fastconnect_6700_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2576 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2577 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2578 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2579 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2580 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-FAST-170225/2581 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2582 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2583 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2584 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2585 |
| **Product: fastconnect_6800_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2586 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2587 |
| Time-of-check Time-of-use (TOCTOU) Race | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-FAST-170225/2588 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Condition | | | | y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2589 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2590 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2591 |
| **Product: fastconnect_6900_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2592 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2593 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2594 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-FAST-170225/2595 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2596 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2597 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2598 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2599 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2600 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2601 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-FAST-170225/2602 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2603 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2604 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2605 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2606 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2607 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2608 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2609 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2610 |
| **Product: fastconnect_7800_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2611 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2612 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2613 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2614 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2615 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-FAST-170225/2616 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2617 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2618 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2619 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2620 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2621 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2622 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2623 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-FAST- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2624 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2625 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2626 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2627 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2628 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2629 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2630 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware | https://docs.qualcomm.com/product/publicres | O-QUA-FAST-170225/2631 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | image during core initialization.<br>**CVE ID: CVE-2024-38414** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2632 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FAST-170225/2633 |
| **Product: flight_rb5_5g_platform_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-FLIG-170225/2634 |
| **Product: immersive_home_214_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2635 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2636 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-IMME-170225/2637 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| **Product: immersive_home_216_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2638 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2639 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2640 |
| **Product: immersive_home_316_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2641 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2642 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2643 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: immersive_home_318_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2644 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2645 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2646 |
| **Product: immersive_home_3210_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2647 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2648 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2649 |
| **Product: immersive_home_326_firmware** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2650 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2651 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IMME-170225/2652 |
| **Product: ipq5010_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2653 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2654 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2655 |
| **Product: ipq5028_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-IPQ5-170225/2656 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2657 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2658 |
| **Product: ipq5300_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2659 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2660 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2661 |
| **Product: ipq5302_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-IPQ5-170225/2662 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2663 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2664 |
| **Product: ipq5312_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2665 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2666 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2667 |
| **Product: ipq5332_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2668 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | O-QUA-IPQ5-170225/2669 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ5-170225/2670 |
| **Product: ipq6000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2671 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2672 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2673 |
| **Product: ipq6010_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2674 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-IPQ6-170225/2675 |

| 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 |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2676 |
| **Product: ipq6018_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2677 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2678 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2679 |
| **Product: ipq6028_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2680 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ6-170225/2681 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | O-QUA-IPQ6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2682 |
| **Product: ipq8070a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2683 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2684 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2685 |
| **Product: ipq8071a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2686 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2687 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command | https://docs.qualcomm.com/product/publicresources/security | O-QUA-IPQ8-170225/2688 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the interface.<br>**CVE ID: CVE-2024-45571** | bulletin/februar y-2025-bulletin.html | |
| **Product: ipq8072a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2689 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2690 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2691 |
| **Product: ipq8074a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2692 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2693 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2694 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: ipq8076a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2695 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2696 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2697 |
| **Product: ipq8076_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2698 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2699 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2700 |
| **Product: ipq8078a_firmware** | | | | | |
| Affected Version(s): - | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2701 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2702 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2703 |
| **Product: ipq8078_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2704 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2705 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2706 |
| **Product: ipq8173_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-IPQ8-170225/2707 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2708 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2709 |
| **Product: ipq8174_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2710 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2711 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ8-170225/2712 |
| **Product: ipq9008_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-IPQ9-170225/2713 |

| 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 |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2714 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2715 |
| **Product: ipq9048_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2716 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2717 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2718 |
| **Product: ipq9554_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2719 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | O-QUA-IPQ9-170225/2720 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2721 |
| **Product: ipq9570_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2722 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2723 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2724 |
| **Product: ipq9574_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2725 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-IPQ9-170225/2726 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-IPQ9-170225/2727 |
| **Product: mdm9628_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-MDM9-170225/2728 |
| **Product: msm8996au_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-MSM8-170225/2729 |
| **Product: qam8255p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2730 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2731 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QAM8-170225/2732 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2733 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2734 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2735 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2736 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2737 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2738 |
| **Product: qam8295p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QAM8-170225/2739 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2740 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2741 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2742 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2743 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2744 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2745 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QAM8-170225/2746 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2747 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2748 |
| **Product: qam8620p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2749 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2750 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2751 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2752 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QAM8-170225/2753 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2754 |
| **Product: qam8650p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2755 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2756 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2757 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2758 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2759 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QAM8-170225/2760 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2761 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2762 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2763 |
| **Product: qam8775p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2764 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2765 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2766 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-QAM8-170225/2767 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2768 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2769 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2770 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2771 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAM8-170225/2772 |
| **Product: qamsrv1h_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2773 |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | O-QUA-QAMS-170225/2774 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2775 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2776 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2777 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2778 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2779 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2780 |
| **Product: qamsrv1m_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 9.8 | Memory corruption while | https://docs.qu | O-QUA-QAMS- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2781 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2782 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2783 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2784 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2785 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2786 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QAMS-170225/2787 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | O-QUA-QAMS-170225/2788 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qca0000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA0-170225/2789 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA0-170225/2790 |
| **Product: qca4024_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA4-170225/2791 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA4-170225/2792 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA4-170225/2793 |
| **Product: qca6174a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2794 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2795 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2796 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2797 |
| **Product: qca6310_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2798 |
| **Product: qca6335_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2799 |
| **Product: qca6391_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2800 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2801 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2802 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2803 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2804 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2805 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2806 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCA6-170225/2807 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45561** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2808 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2809 |
| **Product: qca6420_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2810 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2811 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2812 |
| **Product: qca6421_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2813 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qca6426_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2814 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2815 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2816 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2817 |
| **Product: qca6430_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2818 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2819 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2820 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | level.<br>**CVE ID: CVE-2024-45561** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qca6431_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA6-170225/2821 |
| **Product: qca6436_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA6-170225/2822 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA6-170225/2823 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA6-170225/2824 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA6-170225/2825 |
| **Product: qca6554a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2826 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2827 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2828 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2829 |
| **Product: qca6564au_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2830 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2831 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2832 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | O-QUA-QCA6-170225/2833 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | with invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2834 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2835 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2836 |
| **Product: qca6564a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2837 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2838 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2839 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qca6574au_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2840 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2841 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2842 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2843 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2844 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2845 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCA6-170225/2846 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2847 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2848 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2849 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2850 |
| **Product: qca6574a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2851 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2852 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QCA6-170225/2853 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2854 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2855 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2856 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2857 |
| **Product: qca6574_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2858 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2859 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2860 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2861 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2862 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2863 |
| **Product: qca6584au_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2864 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2865 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2866 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | O-QUA-QCA6-170225/2867 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | with invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2868 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2869 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2870 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2871 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2872 |
| **Product: qca6595au_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2873 |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | O-QUA-QCA6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2874 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2875 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2876 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2877 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2878 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2879 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2880 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2881 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/februar y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2882 |
| **Product: qca6595_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2883 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2884 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2885 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2886 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2887 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when | https://docs.qualcomm.com/pr | O-QUA-QCA6-170225/2888 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2889 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2890 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2891 |
| **Product: qca6678aq_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2892 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2893 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2894 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | O-QUA-QCA6- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2895 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2896 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2897 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2898 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2899 |
| **Product: qca6688aq_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2900 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2901 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2902 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2903 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2904 |
| **Product: qca6696_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2905 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2906 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2907 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCA6-170225/2908 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2909 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2910 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2911 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2912 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2913 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2914 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2915 |
| **Product: qca6698aq_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2916 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2917 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2918 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2919 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2920 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2921 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2922 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | O-QUA-QCA6- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2923 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2924 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2925 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2926 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2927 |
| **Product: qca6777aq_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2928 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2929 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2930 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2931 |
| **Product: qca6787aq_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2932 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2933 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2934 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2935 |
| **Product: qca6797aq_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA6-170225/2936 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2937 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2938 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2939 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2940 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2941 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA6-170225/2942 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCA6-170225/2943 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | y-2025-bulletin.html | |
| **Product: qca8075_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2944 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2945 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2946 |
| **Product: qca8081_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2947 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2948 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2949 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Information disclosure | https://docs.qu | O-QUA-QCA8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2950 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2951 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2952 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2953 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2954 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2955 |
| **Product: qca8082_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2956 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2957 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2958 |
| **Product: qca8084_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2959 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2960 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2961 |
| **Product: qca8085_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2962 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-QCA8-170225/2963 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2964 |
| **Product: qca8337_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2965 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2966 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2967 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2968 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/security bulletin/februar y-2025-bulletin.html | O-QUA-QCA8-170225/2969 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | O-QUA-QCA8-170225/2970 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2971 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2972 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2973 |
| **Product: qca8386_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2974 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2975 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA8-170225/2976 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qca9367_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2977 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2978 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2979 |
| **Product: qca9377_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2980 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2981 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2982 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. | https://docs.qualcomm.com/product/publicres | O-QUA-QCA9-170225/2983 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38416** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qca9888_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2984 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2985 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2986 |
| **Product: qca9889_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2987 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCA9-170225/2988 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCA9-170225/2989 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| **Product: qcc2073_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2990 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2991 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2992 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2993 |
| **Product: qcc2076_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2994 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2995 |
| Buffer Over- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-QCC2- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/2996 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC2-170225/2997 |
| **Product: qcc710_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/2998 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/2999 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3000 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3001 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3002 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3003 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3004 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3005 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCC7-170225/3006 |
| **Product: qcf8000sfp_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3007 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3008 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCF8-170225/3009 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| **Product: qcf8000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3010 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3011 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3012 |
| **Product: qcf8001_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3013 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3014 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCF8-170225/3015 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: qcm4325_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM4-170225/3016 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM4-170225/3017 |
| **Product: qcm4490_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM4-170225/3018 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM4-170225/3019 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM4-170225/3020 |
| **Product: qcm5430_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3021 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3022 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3023 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3024 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3025 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3026 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. **CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3027 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM5-170225/3028 |
| **Product: qcm6125_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 | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3029 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3030 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3031 |
| **Product: qcm6490_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3032 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3033 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3034 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCM6-170225/3035 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3036 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3037 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3038 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM6-170225/3039 |
| **Product: qcm8550_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3040 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3041 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QCM8-170225/3042 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3043 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3044 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3045 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3046 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3047 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCM8-170225/3048 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCM8-170225/3049 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qcn5022_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3050 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3051 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3052 |
| **Product: qcn5024_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3053 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3054 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3055 |
| **Product: qcn5052_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3056 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3057 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3058 |
| **Product: qcn5122_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3059 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3060 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3061 |
| **Product: qcn5124_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 9.8 | Memory corruption while | https://docs.qu | O-QUA-QCN5- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3062 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3063 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3064 |
| **Product: qcn5152_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3065 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3066 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3067 |
| **Product: qcn5154_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QCN5-170225/3068 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3069 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3070 |
| **Product: qcn5164_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3071 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3072 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN5-170225/3073 |
| **Product: qcn6023_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3074 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3075 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3076 |
| **Product: qcn6024_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3077 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3078 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3079 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3080 |
| **Product: qcn6112_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-QCN6-170225/3081 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3082 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3083 |
| **Product: qcn6122_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3084 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3085 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3086 |
| **Product: qcn6132_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCN6-170225/3087 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3088 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3089 |
| **Product: qcn6224_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3090 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3091 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3092 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3093 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCN6-170225/3094 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3095 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3096 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3097 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3098 |
| **Product: qcn6274_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3099 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3100 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QCN6-170225/3101 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3102 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3103 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3104 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3105 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3106 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3107 |
| **Product: qcn6402_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-QCN6-170225/3108 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3109 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3110 |
| **Product: qcn6412_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3111 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3112 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3113 |
| **Product: qcn6422_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCN6-170225/3114 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3115 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3116 |
| **Product: qcn6432_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3117 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3118 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN6-170225/3119 |
| **Product: qcn9000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3120 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | O-QUA-QCN9-170225/3121 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3122 |
| **Product: qcn9011_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3123 |
| **Product: qcn9012_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3124 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3125 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3126 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCN9-170225/3127 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | y-2025-bulletin.html | |
| **Product: qcn9022_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3128 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3129 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3130 |
| **Product: qcn9024_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3131 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3132 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3133 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | O-QUA-QCN9- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | 170225/3134 |
| **Product: qcn9070_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3135 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3136 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3137 |
| **Product: qcn9072_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3138 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/security bulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3139 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QCN9-170225/3140 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | from the interface.<br>**CVE ID: CVE-2024-45571** | bulletin/february-2025-bulletin.html | |
| **Product: qcn9074_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3141 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3142 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3143 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3144 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3145 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3146 |
| **Product: qcn9100_firmware** | | | | | |
| Affected Version(s): - | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3147 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3148 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3149 |
| **Product: qcn9160_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3150 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3151 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3152 |
| **Product: qcn9274_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicres | O-QUA-QCN9-170225/3153 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3154 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3155 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3156 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3157 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCN9-170225/3158 |
| **Product: qcs410_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3159 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down | https://docs.qualcomm.com/pr | O-QUA-QCS4-170225/3160 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3161 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3162 |
| **Product: qcs4490_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3163 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3164 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS4-170225/3165 |
| **Product: qcs5430_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QCS5-170225/3166 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3167 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3168 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3169 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3170 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3171 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3172 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS5-170225/3173 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: qcs610_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3174 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3175 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3176 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3177 |
| **Product: qcs6125_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3178 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3179 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB | https://docs.qualcomm.com/product/publicres | O-QUA-QCS6-170225/3180 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bus error.<br>**CVE ID: CVE-2024-49843** | ources/security bulletin/februar y-2025-bulletin.html | |
| **Product: qcs615_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3181 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3182 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3183 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3184 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3185 |
| **Product: qcs6490_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QCS6-170225/3186 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3187 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3188 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3189 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3190 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3191 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3192 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3193 |
| Use After | 03-Feb-2025 | 7.8 | Memory corruption may | https://docs.qu | O-QUA-QCS6- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3194 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3195 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3196 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS6-170225/3197 |
| **Product: qcs7230_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS7-170225/3198 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS7-170225/3199 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS7-170225/3200 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS7-170225/3201 |
| **Product: qcs8250_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3202 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3203 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3204 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3205 |
| **Product: qcs8300_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3206 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-QCS8-170225/3207 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3208 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3209 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3210 |
| **Product: qcs8550_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3211 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3212 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3213 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | O-QUA-QCS8-170225/3214 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3215 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3216 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3217 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3218 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3219 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS8-170225/3220 |
| **Product: qcs9100_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 9.8 | Memory corruption while | https://docs.qu | O-QUA-QCS9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3221 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS9-170225/3222 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS9-170225/3223 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS9-170225/3224 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS9-170225/3225 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QCS9-170225/3226 |
| **Product: qdu1000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3227 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3228 |
| **Product: qdu1010_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3229 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3230 |
| **Product: qdu1110_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3231 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3232 |
| **Product: qdu1210_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3233 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDU1-170225/3234 |
| **Product: qdx1010_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDX1-170225/3235 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDX1-170225/3236 |
| **Product: qdx1011_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDX1-170225/3237 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QDX1-170225/3238 |
| **Product: qep8111_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QEP8-170225/3239 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QEP8-170225/3240 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QEP8-170225/3241 |
| **Product: qfw7114_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3242 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3243 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3244 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3245 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-QFW7-170225/3246 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3247 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3248 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3249 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3250 |
| **Product: qfw7124_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3251 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3252 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-QFW7-170225/3253 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3254 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3255 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3256 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3257 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3258 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QFW7-170225/3259 |
| **Product: qrb5165m_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-QRB5-170225/3260 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| **Product: qrb5165n_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRB5-170225/3261 |
| **Product: qru1032_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRU1-170225/3262 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRU1-170225/3263 |
| **Product: qru1052_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRU1-170225/3264 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRU1-170225/3265 |
| **Product: qru1062_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | O-QUA-QRU1- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3266 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QRU1-170225/3267 |
| **Product: qsm8250_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QSM8-170225/3268 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QSM8-170225/3269 |
| **Product: qsm8350_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QSM8-170225/3270 |
| **Product: qxm8083_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QXM8-170225/3271 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | O-QUA-QXM8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3272 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-QXM8-170225/3273 |
| **Product: robotics_rb2_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-ROBO-170225/3274 |
| **Product: robotics_rb3_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-ROBO-170225/3275 |
| **Product: robotics_rb5_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-ROBO-170225/3276 |
| **Product: sa6145p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SA61-170225/3277 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3278 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3279 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3280 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3281 |
| **Product: sa6150p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3282 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3283 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SA61-170225/3284 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3285 |
| **Product: sa6155p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3286 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3287 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3288 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3289 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3290 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | O-QUA-SA61-170225/3291 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3292 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3293 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3294 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3295 |
| **Product: sa6155_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA61-170225/3296 |
| **Product: sa7255p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SA72-170225/3297 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3298 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3299 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3300 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3301 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3302 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3303 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA72-170225/3304 |
| **Product: sa7775p_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3305 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3306 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3307 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3308 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3309 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3310 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA77-170225/3311 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-SA77- |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3312 |
| **Product: sa8145p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3313 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3314 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3315 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3316 |
| **Product: sa8150p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3317 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SA81-170225/3318 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization. **CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3319 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3320 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3321 |
| **Product: sa8155p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3322 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3323 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3324 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-SA81-170225/3325 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3326 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3327 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3328 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3329 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3330 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3331 |
| **Product: sa8155_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | O-QUA-SA81-170225/3332 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: sa8195p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3333 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3334 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3335 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3336 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3337 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3338 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | O-QUA-SA81- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3339 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3340 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA81-170225/3341 |
| **Product: sa8255p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3342 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3343 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3344 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3345 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3346 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3347 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3348 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3349 |
| **Product: sa8295p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3350 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3351 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SA82-170225/3352 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3353 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3354 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3355 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3356 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3357 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3358 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA82-170225/3359 |
| **Product: sa8530p_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3360 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3361 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3362 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3363 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3364 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3365 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3366 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: sa8540p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3367 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3368 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3369 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3370 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3371 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3372 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SA85-170225/3373 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3374 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA85-170225/3375 |
| **Product: sa8620p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3376 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3377 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3378 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3379 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SA86-170225/3380 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3381 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3382 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3383 |
| **Product: sa8650p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3384 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3385 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3386 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SA86-170225/3387 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3388 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3389 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3390 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA86-170225/3391 |
| **Product: sa8770p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3392 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3393 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | O-QUA-SA87-170225/3394 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3395 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3396 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3397 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. **CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3398 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3399 |
| **Product: sa8775p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3400 |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | O-QUA-SA87-170225/3401 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3402 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3403 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3404 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3405 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3406 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA87-170225/3407 |
| **Product: sa9000p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 9.8 | Memory corruption while | https://docs.qu | O-QUA-SA90- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3408 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3409 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3410 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3411 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3412 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3413 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3414 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend. | https://docs.qualcomm.com/product/publicres | O-QUA-SA90-170225/3415 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49837** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3416 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3417 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3418 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SA90-170225/3419 |
| **Product: sc8180x-aaab_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3420 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3421 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from | https://docs.qualcomm.com/pr | O-QUA-SC81-170225/3422 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: sc8180x-acaf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3423 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3424 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3425 |
| **Product: sc8180x-ad_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3426 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3427 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SC81-170225/3428 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45561** | y-2025-bulletin.html | |
| **Product: sc8180xp-aaab_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3429 |
| **Product: sc8180xp-acaf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3430 |
| **Product: sc8180xp-ad_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC81-170225/3431 |
| **Product: sc8280xp-abbb_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC82-170225/3432 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC82-170225/3433 |
| Buffer Over- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-SC82- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3434 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC82-170225/3435 |
| **Product: sc8380xp_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3436 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3437 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3438 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3439 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3440 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SC83-170225/3441 |
| **Product: sd670_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD67-170225/3442 |
| **Product: sd675_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD67-170225/3443 |
| **Product: sd855_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD85-170225/3444 |
| **Product: sd865_5g_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD86-170225/3445 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SD86-170225/3446 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/february-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD86-170225/3447 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD86-170225/3448 |
| **Product: sd888_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD88-170225/3449 |
| **Product: sdm429w_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3450 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3451 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3452 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3453 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3454 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. **CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3455 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3456 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands. **CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDM4-170225/3457 |
| **Product: sdx55_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3458 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SDX5-170225/3459 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3460 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3461 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3462 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3463 |
| **Product: sdx57m_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX5-170225/3464 |
| **Product: sdx61_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX6-170225/3465 |
| **Product: sdx65m_firmware** | | | | | |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX6-170225/3466 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX6-170225/3467 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX6-170225/3468 |
| **Product: sdx80m_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX8-170225/3469 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SDX8-170225/3470 |
| **Product: sd_675_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_6-170225/3471 |
| **Product: sd_8cx_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_8-170225/3472 |
| **Product: sd_8_gen1_5g_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_8-170225/3473 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_8-170225/3474 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_8-170225/3475 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SD_8-170225/3476 |
| **Product: sg4150p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SG41-170225/3477 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-SG41- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pointer Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3478 |
| **Product: sg8275p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SG82-170225/3479 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SG82-170225/3480 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SG82-170225/3481 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SG82-170225/3482 |
| **Product: sm4635_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM46-170225/3483 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SM46-170225/3484 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM46-170225/3485 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM46-170225/3486 |
| **Product: sm6370_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM63-170225/3487 |
| **Product: sm6650_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3488 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3489 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3490 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3491 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3492 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3493 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3494 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3495 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM66-170225/3496 |
| **Product: sm7250p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SM72-170225/3497 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: sm7315_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM73-170225/3498 |
| **Product: sm7325p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM73-170225/3499 |
| **Product: sm7635_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3500 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3501 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3502 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SM76-170225/3503 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3504 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3505 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3506 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3507 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3508 |
| **Product: sm7675p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3509 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SM76-170225/3510 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3511 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3512 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3513 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3514 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3515 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3516 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3517 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3518 |
| **Product: sm7675_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3519 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3520 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3521 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3522 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3523 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SM76-170225/3524 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3525 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3526 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3527 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM76-170225/3528 |
| **Product: sm8550p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3529 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3530 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SM85-170225/3531 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3532 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3533 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3534 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3535 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM85-170225/3536 |
| **Product: sm8635p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3537 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SM86-170225/3538 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3539 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3540 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3541 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3542 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3543 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SM86-170225/3544 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025- | O-QUA-SM86-170225/3545 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3546 |
| **Product: sm8635_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3547 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3548 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3549 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3550 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3551 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SM86-170225/3552 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | bulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3553 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3554 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3555 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM86-170225/3556 |
| **Product: sm8750p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3557 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3558 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-SM87-170225/3559 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | in T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3560 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3561 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3562 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3563 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3564 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3565 |
| **Product: sm8750_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to | https://docs.qualcomm.com/pr | O-QUA-SM87-170225/3566 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | invalid frame content.<br>**CVE ID: CVE-2024-45569** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3567 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3568 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3569 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3570 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3571 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3572 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SM87-170225/3573 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SM87-170225/3574 |
| **Product: smart_audio_400_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SMAR-170225/3575 |
| **Product: snapdragon_429_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3576 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3577 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3578 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3579 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3580 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3581 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3582 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3583 |
| **Product: snapdragon_460_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3584 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3585 |
| **Product: snapdragon_480\+_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | O-QUA-SNAP-170225/3586 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3587 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3588 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3589 |
| **Product: snapdragon_480_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3590 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3591 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-SNAP-170225/3592 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user | https://docs.qualcomm.com/pr | O-QUA-SNAP-170225/3593 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| **Product: snapdragon_4_gen_1_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3594 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3595 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3596 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3597 |
| **Product: snapdragon_4_gen_2_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3598 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SNAP-170225/3599 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49834** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3600 |
| **Product: snapdragon_662_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3601 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3602 |
| **Product: snapdragon_670_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3603 |
| **Product: snapdragon_675_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3604 |
| **Product: snapdragon_678_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3605 |
| **Product: snapdragon_680_4g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3606 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3607 |
| **Product: snapdragon_685_4g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3608 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3609 |
| **Product: snapdragon_695_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3610 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3611 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3612 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3613 |
| **Product: snapdragon_765g_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3614 |
| **Product: snapdragon_765_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3615 |
| **Product: snapdragon_768g_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3616 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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_778g\+_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3617 |
| **Product: snapdragon_778g_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3618 |
| **Product: snapdragon_780g_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3619 |
| **Product: snapdragon_782g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3620 |
| **Product: snapdragon_7c\+_gen_3_compute_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3621 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3622 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3623 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3624 |
| **Product: snapdragon_820_automotive_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3625 |
| **Product: snapdragon_845_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3626 |
| **Product: snapdragon_850_mobile_compute_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3627 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: snapdragon_855\+_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3628 |
| **Product: snapdragon_855_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3629 |
| **Product: snapdragon_860_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3630 |
| **Product: snapdragon_865\+_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3631 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3632 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SNAP-170225/3633 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Race Condition | | | **CVE ID: CVE-2024-38418** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3634 |
| **Product: snapdragon_865_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3635 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3636 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3637 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3638 |
| **Product: snapdragon_870_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3639 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3640 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3641 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3642 |
| **Product: snapdragon_888\+_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3643 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3644 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3645 |
| **Product: snapdragon_888_5g_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicres | O-QUA-SNAP-170225/3646 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3647 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3648 |
| **Product: snapdragon_8\+_gen_1_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3649 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3650 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3651 |
| **Product: snapdragon_8\+_gen_2_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SNAP-170225/3652 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3653 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3654 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3655 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3656 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3657 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3658 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3659 |
| **Product: snapdragon_8_gen_1_mobile_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3660 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3661 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. **CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3662 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3663 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3664 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3665 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3666 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3667 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3668 |
| **Product: snapdragon_8_gen_2_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3669 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3670 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3671 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3672 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3673 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3674 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3675 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3676 |
| **Product: snapdragon_8_gen_3_mobile_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3677 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3678 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3679 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SNAP-170225/3680 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3681 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3682 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3683 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3684 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3685 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3686 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3687 |
| Buffer Over- | 03-Feb-2025 | 7.5 | Transient DOS when | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3688 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3689 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3690 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3691 |
| **Product: snapdragon_ar1_gen_1_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3692 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3693 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3694 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3695 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3696 |
| **Product: snapdragon_ar2_gen_1_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3697 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3698 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3699 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3700 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SNAP-170225/3701 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| **Product: snapdragon_auto_4g_modem_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3702 |
| **Product: snapdragon_auto_5g_modem-rf_gen_2_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3703 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3704 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3705 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3706 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3707 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is | https://docs.qualcomm.com/pr | O-QUA-SNAP-170225/3708 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3709 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3710 |
| **Product: snapdragon_w5\+_gen_1_wearable_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3711 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3712 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3713 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3714 |
| Time-of- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| check Time-of-use (TOCTOU) Race Condition | | | parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3715 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3716 |
| **Product: snapdragon_wear_4100\+_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3717 |
| **Product: snapdragon_x24_lte_modem_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3718 |
| **Product: snapdragon_x35_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3719 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3720 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pointer Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3721 |
| **Product: snapdragon_x50_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3722 |
| **Product: snapdragon_x55_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3723 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3724 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3725 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3726 |
| **Product: snapdragon_x62_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 8.8 | Memory corruption while | https://docs.qu | O-QUA-SNAP- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Input Validation | | | configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3727 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3728 |
| **Product: snapdragon_x65_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3729 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3730 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3731 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3732 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3733 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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_x72_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3734 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3735 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3736 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3737 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3738 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. **CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3739 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SNAP-170225/3740 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3741 |
| **Product: snapdragon_x72_5g_modem-rf_system_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3742 |
| **Product: snapdragon_x75_5g_modem-rf_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3743 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3744 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3745 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3746 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | O-QUA-SNAP-170225/3747 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3748 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3749 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3750 |
| **Product: snapdragon_x75_5g_modem-rf_system_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3751 |
| **Product: snapdragon_xr2\+_gen_1_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3752 |
| **Product: snapdragon_xr2_5g_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | O-QUA-SNAP-170225/3753 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3754 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3755 |
| **Product: snapdragon_xr2_5g_platform_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SNAP-170225/3756 |
| **Product: srv1h_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3757 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3758 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SRV1-170225/3759 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3760 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3761 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3762 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3763 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3764 |
| **Product: srv1l_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3765 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-SRV1-170225/3766 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3767 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3768 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3769 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3770 |
| **Product: srv1m_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3771 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3772 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch | https://docs.qualcomm.com/product/publicres | O-QUA-SRV1-170225/3773 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 T2LM info element.<br>**CVE ID: CVE-2024-49839** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3774 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while reading CPU state data during guest VM suspend.<br>**CVE ID: CVE-2024-49837** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3775 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3776 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3777 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SRV1-170225/3778 |
| **Product: ssg2115p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3779 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE | https://docs.qualcomm.com/pr | O-QUA-SSG2-170225/3780 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 invalid length.<br>**CVE ID: CVE-2024-49838** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3781 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3782 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3783 |
| **Product: ssg2125p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3784 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3785 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3786 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-SSG2- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3787 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SSG2-170225/3788 |
| **Product: sw5100p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3789 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3790 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3791 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3792 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3793 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3794 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3795 |
| **Product: sw5100_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3796 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3797 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3798 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3799 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-SW51-170225/3800 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3801 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SW51-170225/3802 |
| **Product: sxr1230p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR1-170225/3803 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR1-170225/3804 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR1-170225/3805 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR1-170225/3806 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-SXR1-170225/3807 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| **Product: sxr2130_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3808 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3809 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3810 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3811 |
| **Product: sxr2230p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3812 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3813 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Memory corruption during | https://docs.qu | O-QUA-SXR2- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3814 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3815 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3816 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3817 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3818 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3819 |
| **Product: sxr2250p_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3820 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3821 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3822 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3823 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3824 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3825 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3826 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3827 |
| **Product: sxr2330p_firmware** | | | | | |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3828 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3829 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3830 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3831 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3832 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3833 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-SXR2-170225/3834 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-SXR2- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3835 |
| **Product: talynplus_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-TALY-170225/3836 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-TALY-170225/3837 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-TALY-170225/3838 |
| **Product: video_collaboration_vc1_platform_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3839 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3840 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-VIDE-170225/3841 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49843** | bulletin/februar y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3842 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3843 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3844 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3845 |
| **Product: video_collaboration_vc3_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3846 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3847 |
| **Product: video_collaboration_vc3_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 | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3848 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3849 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3850 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. **CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3851 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. **CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3852 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor. **CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3853 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3854 |
| Time-of-check Time- | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with | https://docs.qualcomm.com/pr | O-QUA-VIDE-170225/3855 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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-use (TOCTOU) Race Condition | | | hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3856 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3857 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3858 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3859 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3860 |
| **Product: video_collaboration_vc5_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3861 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| **Product: video_collaboration_vc5_platform_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3862 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3863 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VIDE-170225/3864 |
| **Product: vision_intelligence_300_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VISI-170225/3865 |
| **Product: vision_intelligence_400_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VISI-170225/3866 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VISI-170225/3867 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-VISI-170225/3868 |
| **Product: wcd9326_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3869 |
| **Product: wcd9335_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3870 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3871 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3872 |
| **Product: wcd9340_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3873 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3874 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3875 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3876 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3877 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3878 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3879 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3880 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is | https://docs.qualcomm.com/pr | O-QUA-WCD9-170225/3881 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3882 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3883 |
| **Product: wcd9341_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3884 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3885 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3886 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3887 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-WCD9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Pointer Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3888 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3889 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3890 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3891 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3892 |
| **Product: wcd9370_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3893 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3894 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3895 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3896 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3897 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3898 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3899 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3900 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3901 |
| Time-of-check Time- | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with | https://docs.qualcomm.com/pr | O-QUA-WCD9-170225/3902 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| of-use (TOCTOU) Race Condition | | | hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3903 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3904 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3905 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3906 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3907 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3908 |
| **Product: wcd9375_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper | 03-Feb-2025 | 9.8 | Memory corruption while | https://docs.qu | O-QUA-WCD9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3909 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3910 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3911 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3912 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3913 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3914 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3915 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicres | O-QUA-WCD9-170225/3916 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3917 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3918 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. **CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3919 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3920 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3921 |
| **Product: wcd9378_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3922 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame | https://docs.qualcomm.com/pr | O-QUA-WCD9-170225/3923 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3924 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3925 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3926 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3927 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3928 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3929 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCD9-170225/3930 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49843** | bulletin/february-2025-bulletin.html | |
| **Product: wcd9380_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3931 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3932 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. **CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3933 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. **CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3934 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality. **CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3935 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. **CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3936 |
| Time-of-check Time-of-use | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. | https://docs.qualcomm.com/product/publicres | O-QUA-WCD9-170225/3937 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| (TOCTOU) Race Condition | | | **CVE ID: CVE-2024-38418** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3938 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3939 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. **CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3940 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. **CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3941 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer. **CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3942 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. **CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCD9-170225/3943 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WCD9-170225/3944 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3945 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3946 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3947 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3948 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3949 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3950 |
| **Product: wcd9385_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCD9-170225/3951 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45569** | bulletin/february-2025-bulletin.html | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3952 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3953 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3954 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3955 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3956 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3957 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WCD9-170225/3958 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3959 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3960 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3961 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3962 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3963 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3964 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3965 |
| Use After | 03-Feb-2025 | 6.6 | Memory corruption while | https://docs.qu | O-QUA-WCD9- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Free | | | registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3966 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3967 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3968 |
| **Product: wcd9390_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3969 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3970 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3971 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3972 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3973 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3974 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3975 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3976 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3977 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3978 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3979 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is | https://docs.qualcomm.com/pr | O-QUA-WCD9-170225/3980 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3981 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3982 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3983 |
| **Product: wcd9395_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3984 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3985 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3986 |
| Buffer Over- | 03-Feb-2025 | 8.2 | Information disclosure | https://docs.qu | O-QUA-WCD9- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/3987 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3988 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3989 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3990 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3991 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3992 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3993 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB | https://docs.qualcomm.com/product/publicres | O-QUA-WCD9-170225/3994 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | bus error.<br>**CVE ID: CVE-2024-49843** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3995 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3996 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3997 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCD9-170225/3998 |
| **Product: wcn3610_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/3999 |
| **Product: wcn3620_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WCN3-170225/4000 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4001 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4002 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4003 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4004 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4005 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4006 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4007 |
| **Product: wcn3660b_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): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4008 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4009 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4010 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4011 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4012 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4013 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4014 |
| Buffer Over- | 03-Feb-2025 | 6.1 | Information disclosure | https://docs.qu | O-QUA-WCN3- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| read | | | during audio playback.<br>**CVE ID: CVE-2024-38416** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/4015 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4016 |
| **Product: wcn3680b_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4017 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4018 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4019 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4020 |
| **Product: wcn3950_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCN3-170225/4021 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-38420** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4022 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4023 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4024 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4025 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4026 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4027 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WCN3-170225/4028 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4029 |
| **Product: wcn3980_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4030 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4031 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4032 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4033 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4034 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WCN3-170225/4035 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49843** | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4036 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4037 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4038 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4039 |
| **Product: wcn3988_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4040 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4041 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCN3-170225/4042 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4043 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4044 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4045 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4046 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4047 |
| **Product: wcn3990_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN3-170225/4048 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length. | https://docs.qualcomm.com/product/publicres | O-QUA-WCN3-170225/4049 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49838** | ources/security bulletin/februar y-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN3-170225/4050 |
| **Product: wcn6450_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN6-170225/4051 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN6-170225/4052 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN6-170225/4053 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN6-170225/4054 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar y-2025-bulletin.html | O-QUA-WCN6-170225/4055 |
| Untrusted Pointer | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL | https://docs.qualcomm.com/pr | O-QUA-WCN6-170225/4056 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4057 |
| **Product: wcn6650_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4058 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4059 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4060 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4061 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4062 |
| Untrusted | 03-Feb-2025 | 7.8 | Memory corruption can | https://docs.qu | O-QUA-WCN6- |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 Dereference | | | occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/4063 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4064 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4065 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4066 |
| **Product: wcn6740_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4067 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4068 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4069 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: wcn6755_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4070 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4071 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4072 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4073 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4074 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4075 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WCN6-170225/4076 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4077 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4078 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN6-170225/4079 |
| **Product: wcn7860_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4080 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4081 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4082 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WCN7-170225/4083 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4084 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4085 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4086 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4087 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4088 |
| **Product: wcn7861_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4089 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCN7-170225/4090 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49839** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4091 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4092 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4093 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4094 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4095 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4096 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WCN7-170225/4097 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45571** | bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4098 |
| **Product: wcn7880_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4099 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4100 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4101 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4102 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4103 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WCN7-170225/4104 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45584** | bulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4105 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4106 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4107 |
| **Product: wcn7881_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4108 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4109 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4110 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used. | https://docs.qualcomm.com/product/publicres | O-QUA-WCN7-170225/4111 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49833** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4112 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4113 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4114 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4115 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4116 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WCN7-170225/4117 |
| **Product: wsa8810_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor | https://docs.qualcomm.com/pr | O-QUA-WSA8-170225/4118 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation | | | based input virtual device.<br>**CVE ID: CVE-2024-38420** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4119 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4120 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4121 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4122 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4123 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4124 |
| Time-of-check Time-of-use (TOCTOU) | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WSA8-170225/4125 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | | | buffer.<br>**CVE ID: CVE-2024-45560** | bulletin/february-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4126 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4127 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4128 |
| **Product: wsa8815_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4129 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4130 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4131 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal | https://docs.qualcomm.com/product/publicres | O-QUA-WSA8-170225/4132 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | ources/security bulletin/februar y-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4133 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4134 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4135 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4136 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4137 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4138 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WSA8-170225/4139 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| **Product: wsa8830_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4140 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4141 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4142 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4143 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4144 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4145 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WSA8-170225/4146 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-49832** | bulletin/february-2025-bulletin.html | |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4147 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4148 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4149 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4150 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4151 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4152 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WSA8-170225/4153 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4154 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4155 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4156 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4157 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware image during core initialization.<br>**CVE ID: CVE-2024-38414** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4158 |
| **Product: wsa8832_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4159 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WSA8-170225/4160 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4161 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4162 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4163 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4164 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4165 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4166 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4167 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while parsing the memory map info in IOCTL calls. **CVE ID: CVE-2024-38418** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4168 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel . **CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4169 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface. **CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4170 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem. **CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4171 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback. **CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4172 |
| **Product: wsa8835_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content. **CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4173 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device. **CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WSA8-170225/4174 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | | bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4175 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4176 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4177 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4178 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4179 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4180 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4181 |
| Time-of- | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-WSA8- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| check Time-of-use (TOCTOU) Race Condition | | | parsing the memory map info in IOCTL calls.<br>**CVE ID: CVE-2024-38418** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/4182 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4183 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4184 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4185 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4186 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4187 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4188 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing information on firmware | https://docs.qualcomm.com/product/publicres | O-QUA-WSA8-170225/4189 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | image during core initialization.<br>**CVE ID: CVE-2024-38414** | ources/security bulletin/februar y-2025-bulletin.html | |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure during audio playback.<br>**CVE ID: CVE-2024-38416** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4190 |
| Buffer Over-read | 03-Feb-2025 | 6.1 | Information disclosure while processing IO control commands.<br>**CVE ID: CVE-2024-38417** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4191 |
| **Product: wsa8840_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4192 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4193 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4194 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4195 |
| Improper Validation of | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when | https://docs.qualcomm.com/pr | O-QUA-WSA8-170225/4196 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Array Index | | | an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | oduct/publicresources/securitybulletin/february-2025-bulletin.html | |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4197 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4198 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4199 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4200 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4201 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4202 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID. | https://docs.qualcomm.com/product/publicresources/security | O-QUA-WSA8-170225/4203 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45573** | bulletin/february-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4204 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4205 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4206 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4207 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4208 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4209 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WSA8-170225/4210 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: wsa8845h_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4211 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4212 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4213 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4214 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4215 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4216 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level. | https://docs.qualcomm.com/product/publicresources/securitybulletin/februar | O-QUA-WSA8-170225/4217 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-45561** | y-2025-bulletin.html | |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4218 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4219 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4220 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4221 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4222 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4223 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4224 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4225 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4226 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4227 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4228 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4229 |
| **Product: wsa8845_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Validation of Array Index | 03-Feb-2025 | 9.8 | Memory corruption while parsing the ML IE due to invalid frame content.<br>**CVE ID: CVE-2024-45569** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4230 |
| Improper Input Validation | 03-Feb-2025 | 8.8 | Memory corruption while configuring a Hypervisor based input virtual device.<br>**CVE ID: CVE-2024-38420** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025- | O-QUA-WSA8-170225/4231 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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 | 03-Feb-2025 | 8.2 | Information disclosure while parsing the OCI IE with invalid length.<br>**CVE ID: CVE-2024-49838** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4232 |
| Buffer Over-read | 03-Feb-2025 | 8.2 | Memory corruption during management frame processing due to mismatch in T2LM info element.<br>**CVE ID: CVE-2024-49839** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4233 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption while Invoking IOCTL calls from user-space to validate FIPS encryption or decryption functionality.<br>**CVE ID: CVE-2024-49840** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4234 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while processing IOCTL from user space to handle GPU AHB bus error.<br>**CVE ID: CVE-2024-49843** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4235 |
| Untrusted Pointer Dereference | 03-Feb-2025 | 7.8 | Memory corruption can occur when a compat IOCTL call is followed by a normal IOCTL call from userspace.<br>**CVE ID: CVE-2024-45584** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4236 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption in Camera due to unusually high number of nodes passed to AXI port.<br>**CVE ID: CVE-2024-49832** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4237 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption can occur in the camera when an invalid CID is used.<br>**CVE ID: CVE-2024-49833** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4238 |
| Improper | 03-Feb-2025 | 7.8 | Memory corruption while | https://docs.qu | O-QUA-WSA8- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Validation of Array Index | | | power-up or power-down sequence of the camera sensor.<br>**CVE ID: CVE-2024-49834** | alcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | 170225/4239 |
| Time-of-check Time-of-use (TOCTOU) Race Condition | 03-Feb-2025 | 7.8 | Memory corruption while taking a snapshot with hardware encoder due to unvalidated userspace buffer.<br>**CVE ID: CVE-2024-45560** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4240 |
| Buffer Over-read | 03-Feb-2025 | 7.8 | Memory corruption while handling IOCTL call from user-space to set latency level.<br>**CVE ID: CVE-2024-45561** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4241 |
| Improper Validation of Array Index | 03-Feb-2025 | 7.8 | Memory corruption while validating number of devices in Camera kernel .<br>**CVE ID: CVE-2024-45582** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4242 |
| Use of Out-of-range Pointer Offset | 03-Feb-2025 | 7.8 | Memory corruption may occour while generating test pattern due to negative indexing of display ID.<br>**CVE ID: CVE-2024-45573** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4243 |
| Use After Free | 03-Feb-2025 | 7.8 | Memory corruption may occour occur when stopping the WLAN interface after processing a WMI command from the interface.<br>**CVE ID: CVE-2024-45571** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4244 |
| Buffer Over-read | 03-Feb-2025 | 7.5 | Transient DOS when registration accept OTA is received with incorrect ciphering key data IE in modem.<br>**CVE ID: CVE-2024-38404** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4245 |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while registering a buffer from user-space to kernel-space | https://docs.qualcomm.com/product/publicres | O-QUA-WSA8-170225/4246 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | using IOCTL calls.<br>**CVE ID: CVE-2024-38411** | ources/security bulletin/februar y-2025-bulletin.html | |
| Use After Free | 03-Feb-2025 | 6.6 | Memory corruption while invoking IOCTL calls from user-space to kernel-space to handle session errors.<br>**CVE ID: CVE-2024-38412** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4247 |
| Improper Input Validation | 03-Feb-2025 | 6.6 | Memory corruption while processing frame packets.<br>**CVE ID: CVE-2024-38413** | https://docs.qualcomm.com/product/publicresources/securitybulletin/february-2025-bulletin.html | O-QUA-WSA8-170225/4248 |
| **Vendor: Samsung** | | | | | |
| **Product: android** | | | | | |
| Affected Version(s): 12.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing buffer storing the decoded video frames in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20881** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4249 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in decoding frame buffer in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20890** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4250 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing uninitialized memory for svc1td in libsthmbc.so prior to SMR Jan-2025 Release 1 allows | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=0 | O-SAM-ANDR-170225/4251 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20882** | 1 | |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in handling the block size for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20888** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4252 |
| Out-of-bounds Write | 04-Feb-2025 | 6.4 | Out-of-bounds write in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20885** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4253 |
| Out-of-bounds Write | 04-Feb-2025 | 6.3 | Out-of-bounds write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20904** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4254 |
| Out-of-bounds Read | 04-Feb-2025 | 6.3 | Out-of-bounds read and write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to read and write out-of-bounds memory.<br>**CVE ID: CVE-2025-20905** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4255 |
| N/A | 04-Feb-2025 | 6 | Improper privilege management in Samsung Find prior to SMR Feb-2025 Release 1 allows local privileged attackers to disable Samsung Find.<br>**CVE ID: CVE-2025-20907** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4256 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Out-of-bounds Write | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20889** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4257 |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream of video thumbnails in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20891** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4258 |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in accessing table used for svp8t in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20887** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4259 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in SoundPicker prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20883** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4260 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in Samsung Message prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20884** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4261 |
| Insecure | 04-Feb-2025 | 4.1 | Inclusion of sensitive | https://security. | O-SAM-ANDR- |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Storage of Sensitive Information | | | information in test code in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to get test key.<br>**CVE ID: CVE-2025-20886** | samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | 170225/4262 |
| Affected Version(s): 13.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing buffer storing the decoded video frames in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20881** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4263 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing uninitialized memory for svc1td in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20882** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4264 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in decoding frame buffer in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20890** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4265 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in handling the block size for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4266 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20888** | | |
| Out-of-bounds Write | 04-Feb-2025 | 6.4 | Out-of-bounds write in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20885** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4267 |
| Out-of-bounds Write | 04-Feb-2025 | 6.3 | Out-of-bounds write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20904** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4268 |
| Out-of-bounds Read | 04-Feb-2025 | 6.3 | Out-of-bounds read and write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to read and write out-of-bounds memory.<br>**CVE ID: CVE-2025-20905** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4269 |
| N/A | 04-Feb-2025 | 6 | Improper privilege management in Samsung Find prior to SMR Feb-2025 Release 1 allows local privileged attackers to disable Samsung Find.<br>**CVE ID: CVE-2025-20907** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4270 |
| N/A | 04-Feb-2025 | 5.9 | Protection Mechanism Failure in bootloader prior to SMR Jan-2025 Release 1 allows physical attackers to allow to execute fastboot command. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20892** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4271 |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in accessing table used for svp8t in libsthmbc.so prior to SMR Jan-2025 Release 1 | https://security.samsungmobile.com/securityUpdate.smsb?year= | O-SAM-ANDR-170225/4272 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20887** | 2025&month=01 | |
| Out-of-bounds Write | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20889** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4273 |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream of video thumbnails in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20891** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4274 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in SoundPicker prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20883** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4275 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in Samsung Message prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20884** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4276 |
| Insecure Storage of Sensitive Information | 04-Feb-2025 | 4.1 | Inclusion of sensitive information in test code in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=0 | O-SAM-ANDR-170225/4277 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | get test key.<br>**CVE ID: CVE-2025-20886** | 1 | |
| Affected Version(s): 14.0 | | | | | |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing buffer storing the decoded video frames in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20881** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4278 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in accessing uninitialized memory for svc1td in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20882** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4279 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in decoding frame buffer in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20890** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4280 |
| Out-of-bounds Write | 04-Feb-2025 | 7 | Out-of-bounds write in handling the block size for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to execute arbitrary code with privilege. User interaction is required for triggering this vulnerability. | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4281 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2025-20888** | | |
| Out-of-bounds Write | 04-Feb-2025 | 6.4 | Out-of-bounds write in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20885** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4282 |
| Out-of-bounds Write | 04-Feb-2025 | 6.3 | Out-of-bounds write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to cause memory corruption.<br>**CVE ID: CVE-2025-20904** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4283 |
| Out-of-bounds Read | 04-Feb-2025 | 6.3 | Out-of-bounds read and write in mPOS TUI trustlet prior to SMR Feb-2025 Release 1 allows local privileged attackers to read and write out-of-bounds memory.<br>**CVE ID: CVE-2025-20905** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4284 |
| N/A | 04-Feb-2025 | 6 | Improper privilege management in Samsung Find prior to SMR Feb-2025 Release 1 allows local privileged attackers to disable Samsung Find.<br>**CVE ID: CVE-2025-20907** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=02 | O-SAM-ANDR-170225/4285 |
| N/A | 04-Feb-2025 | 5.9 | Protection Mechanism Failure in bootloader prior to SMR Jan-2025 Release 1 allows physical attackers to allow to execute fastboot command. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20892** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4286 |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream of video thumbnails in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4287 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20891** | | |
| Out-of-bounds Read | 04-Feb-2025 | 5.3 | Out-of-bounds read in accessing table used for svp8t in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20887** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4288 |
| Out-of-bounds Write | 04-Feb-2025 | 5.3 | Out-of-bounds read in decoding malformed bitstream for smp4vtd in libsthmbc.so prior to SMR Jan-2025 Release 1 allows local attackers to read arbitrary memory. User interaction is required for triggering this vulnerability.<br>**CVE ID: CVE-2025-20889** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4289 |
| N/A | 04-Feb-2025 | 5.1 | Improper access control in NotificationManager prior to SMR Jan-2025 Release 1 allows local attackers to change the configuration of notifications.<br>**CVE ID: CVE-2025-20893** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4290 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in SoundPicker prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20883** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4291 |
| N/A | 04-Feb-2025 | 4.6 | Improper access control in Samsung Message prior to SMR Jan-2025 Release 1 allows physical attackers to access data across multiple user profiles.<br>**CVE ID: CVE-2025-20884** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4292 |

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

* stands for all versions

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Insecure Storage of Sensitive Information | 04-Feb-2025 | 4.1 | Inclusion of sensitive information in test code in softsim TA prior to SMR Jan-2025 Release 1 allows local privileged attackers to get test key.<br>**CVE ID: CVE-2025-20886** | https://security.samsungmobile.com/securityUpdate.smsb?year=2025&month=01 | O-SAM-ANDR-170225/4293 |
| **Vendor: Zyxel** | | | | | |
| **Product: sbg3300-n000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-SBG3-170225/4294 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-SBG3-170225/4295 |
| **Product: sbg3300-nb00_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralizati | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** | https://www.zyxel.com/global/ | O-ZYX-SBG3-170225/4296 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Special Elements used in an OS Command ('OS Command Injection') | | | A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-SBG3-170225/4297 |
| **Product: sbg3500-n000_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-SBG3-170225/4298 |
| Improper | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN | https://www.zy | O-ZYX-SBG3- |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Neutralization of Special Elements used in an OS Command ('OS Command Injection') | | | ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | xel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | 170225/4299 |
| **Product: sbg3500-nb00_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-SBG3-170225/4300 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe- | O-ZYX-SBG3-170225/4301 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | **CVE ID: CVE-2024-40891** | 02-04-2025 | |
| **Product: vmg1312-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. **CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG1-170225/4302 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request. **CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG1-170225/4303 |
| **Product: vmg1312-b10b_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure- | O-ZYX-VMG1-170225/4304 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG1-170225/4305 |
| **Product: vmg1312-b10e_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG1-170225/4306 |
| Improper Neutralization of Special Elements used in an OS Command ('OS | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command- | O-ZYX-VMG1-170225/4307 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| Command Injection') | | | version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| **Product: vmg3312-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG3-170225/4308 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG3-170225/4309 |
| **Product: vmg3313-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection | https://www.zyxel.com/global/en/support/security- | O-ZYX-VMG3-170225/4310 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| used in an OS Command ('OS Command Injection') | | | vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG3-170225/4311 |
| **Product: vmg3926-b10b_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG3-170225/4312 |
| Improper Neutralizati | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** | https://www.zyxel.com/global/ | O-ZYX-VMG3-170225/4313 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| on of Special Elements used in an OS Command ('OS Command Injection') | | | A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| **Product: vmg4325-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG4-170225/4314 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG4-170225/4315 |

| CVSSv3 Scoring Scale | 0-1 | 1-2 | 2-3 | 3-4 | 4-5 | 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: vmg4380-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet. **CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG4-170225/4316 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request. **CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG4-170225/4317 |
| **Product: vmg8324-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED** A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials- | O-ZYX-VMG8-170225/4318 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG8-170225/4319 |
| **Product: vmg8924-b10a_firmware** | | | | | |
| Affected Version(s): - | | | | | |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the management commands of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device via Telnet.<br>**CVE ID: CVE-2024-40891** | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | O-ZYX-VMG8-170225/4320 |
| Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | 04-Feb-2025 | 8.8 | **UNSUPPORTED WHEN ASSIGNED**<br>A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to | https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default- | O-ZYX-VMG8-170225/4321 |

| Weakness | Publish Date | CVSSv3 | Description & CVE ID | Patch | NCIIPC ID |
|---|---|---|---|---|---|
| | | | execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.<br>**CVE ID: CVE-2024-40890** | credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025 | |

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

* stands for all versions