

# May 2026 Security Bulletin

**Published: 05/04/2026**

This security bulletin is intended to help Qualcomm Technologies, Inc. (QTI) customers incorporate security updates in launched or upcoming devices. This document includes (i) a description of security issues that have been addressed in QTI's proprietary code and (ii) links to publicly available code where security issues have been addressed.

Please reach out to [securitybulletin@qti.qualcomm.com](mailto:securitybulletin@qti.qualcomm.com) for any questions related to this bulletin.

## Table of Contents

<a href="#">Announcements</a>	
<a href="#">Acknowledgements</a>	
<a href="#">Proprietary Software Issues</a>	
<a href="#">Open Source Software Issues</a>	
<a href="#">Industry Coordination</a>	

## Announcements

None

## Acknowledgements

We would like to thank these researchers for their contributions in reporting these issues to us.

CVE-2026-25254,CVE-2026-25255	Aaron Thacker (@thackeraaron)
CVE-2026-25262	Alexander Kozlov from Kaspersky ICS CERT
CVE-2026-25293	Tobias Scharnowski (@ScepticCtf), Felix Buchmann, and Krist
CVE-2025-47404	kmalloc1k (kmalloc1k)
CVE-2025-47405,CVE-2025-47406	heiheidada
CVE-2025-47407	Maher Azzouzi
CVE-2026-25266	Nicola Stauffer

## Proprietary Software Issues

The tables below summarize security vulnerabilities that were addressed through proprietary software

This table lists high impact security vulnerabilities. Patches are being actively shared with OEMs, who have been notified and strongly recommended to deploy those patches on released devices as soon as possible. Please contact the device manufacturer for information on the patching status of released devices.

Public ID	Security Rating	CVSS Rating	Technology Area	Date Reported
<a href="#">CVE-2026-25254</a>	Critical	Critical	Qualcomm Software Center	01/09/2026
<a href="#">CVE-2026-25262</a>	Critical	Medium	Boot	03/14/2025
<a href="#">CVE-2026-25293</a>	Critical	Critical	PLC FW	02/19/2026
<a href="#">CVE-2025-47401</a>	High	Medium	WLAN HAL	Internal
<a href="#">CVE-2025-47403</a>	High	Medium	WLAN Firmware	Internal

Public ID	Security Rating	CVSS Rating	Technology Area	Date Reported
<a href="#">CVE-2025-47408</a>	High	High	WINBLAST-POWER	Internal
<a href="#">CVE-2026-25255</a>	High	High	Qualcomm Software Center	12/29/2025

This table lists moderate security vulnerabilities. OEMs have been notified and encouraged to patch these issues.

Public ID	Security Rating	CVSS Rating	Technology Area	Date Reported
<a href="#">CVE-2025-47405</a>	Medium	High	Camera	06/01/2025
<a href="#">CVE-2025-47406</a>	Medium	Medium	DSP Service	06/07/2025
<a href="#">CVE-2026-25266</a>	Medium	Medium	Windows WLAN Host	12/22/2025

## CVE-2026-25254

CVE ID	CVE-2026-25254
Title	Improper authorization in Qualcomm Software Center
Description	Improper authorization leads to Remote Code Execution via SocketIO inter
Technology Area	Qualcomm Software Center
Vulnerability Type	CWE-285: Improper Authorization
Access Vector	Remote
Security Rating	Critical
CVSS Rating	Critical
CVSS Score	9.8
CVSS String	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Date Reported	2026/01/09
Customer Notified Date	2026/02/13
Affected Chipsets*	QSCv1.17.1, QSCv1.19.1, QSCv1.21.0

## CVE-2026-25262

CVE ID	CVE-2026-25262
Title	Write-what-where Condition in Primary Bootloader
Description	Memory corruption while processing a crafted ELF file in the Primary Boot
Technology Area	Boot
Vulnerability Type	CWE-123: Write-what-where Condition
Access Vector	Local
Security Rating	Critical
CVSS Rating	Medium
CVSS Score	6.9
CVSS String	CVSS:3.1/AV:P/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H
Date Reported	2025/03/14
Customer Notified Date	2026/04/20
Affected Chipsets*	MDM9x07, MDM9x45, MDM9x55, MDM9x65, MSM8909, MSM8916, MSM

## CVE-2026-25293

CVE ID	CVE-2026-25293
Title	Incorrect authorization in PLC FW
Description	Buffer overflow due to incorrect authorization in PLC FW
Technology Area	PLC FW
Vulnerability Type	CWE-863
Access Vector	Remote
Security Rating	Critical
CVSS Rating	Critical
CVSS Score	9.6

CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Date Reported	2026/02/19
Customer Notified Date	2026/04/24
Affected Chipsets*	QCA7005

## CVE-2025-47401

CVE ID	CVE-2025-47401
Title	Buffer Over-read in WLAN HAL
Description	Transient DOS when processing target power rate tables during channel c
Technology Area	WLAN HAL
Vulnerability Type	CWE-126 Buffer Over-read
Access Vector	Remote
Security Rating	High
CVSS Rating	Medium
CVSS Score	6.5
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Date Reported	Internal
Customer Notified Date	2025/11/03
Affected Chipsets*	AR8035, Cologne, CQ7790, CQ8725S, CQ8750M, FastConnect 6200, Fast

## CVE-2025-47403

CVE ID	CVE-2025-47403
Title	Buffer Over-read in WLAN Firmware
Description	Transient DOS when processing a malformed Fast Transition response fra
Technology Area	WLAN Firmware

Vulnerability Type	CWE-126 Buffer Over-read
Access Vector	Remote
Security Rating	High
CVSS Rating	Medium
CVSS Score	6.5
CVSS String	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Date Reported	Internal
Customer Notified Date	2025/11/03
Affected Chipsets*	AR8035, Cologne, CQ7790, CQ8725S, CQ8750M, CSR8811, FastConnect

## CVE-2025-47408

CVE ID	CVE-2025-47408
Title	Untrusted Pointer Dereference in Power Optimization Firmware
Description	Memory corruption when another driver calls an IOCTL with invalid input/c
Technology Area	WINBLAST-POWER
Vulnerability Type	CWE-822 Untrusted Pointer Dereference
Access Vector	Local
Security Rating	High
CVSS Rating	High
CVSS Score	7.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Date Reported	Internal
Customer Notified Date	2025/11/03
Affected Chipsets*	FastConnect 6200, FastConnect 6900, FastConnect 7800, IQX5121, IQX7

## CVE-2026-25255

CVE ID	CVE-2026-25255
Title	Exposed function in Qualcomm Package Manager and Qualcomm Software
Description	Exposed dangerous function lead to privilege escalation via gRPC server.
Technology Area	Qualcomm Software Center
Vulnerability Type	CWE-749: Exposed Dangerous Method or Function
Access Vector	Remote
Security Rating	High
CVSS Rating	High
CVSS Score	8.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Date Reported	2025/12/29
Customer Notified Date	2026/02/13
Affected Chipsets*	QSCv1.17.1, QSCv1.19.1, QSCv1.21.0, QPMv3.0.125.4, QPMv3.0.126.7, C

## CVE-2025-47405

CVE ID	CVE-2025-47405
Title	Untrusted Pointer Dereference in Camera
Description	Memory corruption when processing camera sensor input/output control c
Technology Area	Camera
Vulnerability Type	CWE-822 Untrusted Pointer Dereference
Access Vector	Local
Security Rating	Medium
CVSS Rating	High
CVSS Score	7.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Date Reported	2025/06/01
Customer Notified Date	2025/11/03
Affected Chipsets*	FastConnect 6900, FastConnect 7800, IQX5121, IQX7181, QCA0000, SC8

## CVE-2025-47406

CVE ID	CVE-2025-47406
Title	Buffer Over-read in DSP Service
Description	Information Disclosure while processing IOCTL handler callbacks without
Technology Area	DSP Service
Vulnerability Type	CWE-126 Buffer Over-read
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.1
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L
Date Reported	2025/06/07
Customer Notified Date	2025/11/03
Affected Chipsets*	Cologne, FastConnect 6700, FastConnect 6900, FastConnect 7800, IQX51

## CVE-2026-25266

CVE ID	CVE-2026-25266
Title	Exposed dangerous function in windows host
Description	Memory corruption while processing IOCTL command when device is in p
Technology Area	Windows WLAN Host
Vulnerability Type	CWE-749: Exposed Dangerous Method or Function

Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	5.5
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
Date Reported	2025/12/22
Customer Notified Date	2026/04/06
Affected Chipsets*	Cologne, FastConnect 6900, FastConnect 7800, SC8380XP, Snapdragon A

\*The list of affected chipsets may not be complete. For latest information, device OEMs can contact QTI directly at [www.qualcomm.com/support](http://www.qualcomm.com/support).

## Open Source Software Issues

The tables below summarize security vulnerabilities that were addressed through open source software

This table lists high impact security vulnerabilities. Patches are being actively shared with OEMs, who have been notified and strongly recommended to deploy those patches on released devices as soon as possible. Please contact the device manufacturer for information on the patching status of released devices.

Public ID	Security Rating	CVSS Rating	Technology Area	Date Reported
<a href="#">CVE-2026-24082</a>	High	High	Automotive GPU	Internal

This table lists moderate security vulnerabilities. OEMs have been notified and encouraged to patch these issues.

Public ID	Security Rating	CVSS Rating	Technology Area	Date Reported
<a href="#">CVE-2025-47404</a>	Medium	Medium	Automotive Audio	06/07/2025
<a href="#">CVE-2025-47407</a>	Medium	High	DSP Service	06/27/2025

## CVE-2026-24082

CVE ID	CVE-2026-24082
Title	Use After Free in Automotive GPU
Description	Memory Corruption when copying data from a freed source while executin
Technology Area	Automotive GPU
Vulnerability Type	CWE-416 Use After Free
Access Vector	Local
Security Rating	High
CVSS Rating	High
CVSS Score	7.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Date Reported	Internal
Customer Notified Date	2026/02/02
Affected Chipsets*	AR8031, AR8035, CSRA6620, CSRA6640, FastConnect 6200, FastConnec
Patch**	<ul style="list-style-type: none"> <li><a href="https://git.codelinaro.org/clo/la/kernel/msm-5.15/-/commit/e778bf9541f">https://git.codelinaro.org/clo/la/kernel/msm-5.15/-/commit/e778bf9541f</a></li> </ul>

## CVE-2025-47404

CVE ID	CVE-2025-47404
Title	Buffer Copy Without Checking Size of Input in Automotive Audio
Description	Memory corruption when dynamically changing the size of a previously all
Technology Area	Automotive Audio
Vulnerability Type	CWE-120 Buffer Copy Without Checking Size of Input ('Classic Buffer Over
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium

CVSS Score	6.5
CVSS String	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L
Date Reported	2025/06/07
Customer Notified Date	2025/11/03
Affected Chipsets*	5G Fixed Wireless Access Platform, AR8031, AR8035, C-V2X 9150, CSRA6
Patch**	<ul style="list-style-type: none"> <li><a href="https://git.codelinaro.org/clo/la/platform/vendor/opensource/audio-kern">https://git.codelinaro.org/clo/la/platform/vendor/opensource/audio-kern</a></li> </ul>

## CVE-2025-47407

CVE ID	CVE-2025-47407
Title	Time-of-check Time-of-use (TOCTOU) Race Condition in DSP Service
Description	Memory corruption while creating a process on the digital signal process
Technology Area	DSP Service
Vulnerability Type	CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition
Access Vector	Local
Security Rating	Medium
CVSS Rating	High
CVSS Score	7.8
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Date Reported	2025/06/27
Customer Notified Date	2025/11/03
Affected Chipsets*	CQ7790, CQ8725S, FastConnect 6200, FastConnect 6700, FastConnect 6
Patch**	<ul style="list-style-type: none"> <li><a href="https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-l">https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-l</a></li> </ul>

\* The list of affected chipsets may not be complete. For latest information, device OEMs can contact QTI directly at [www.qualcomm.com/support](http://www.qualcomm.com/support).

\*\* Data is generated only at the time of bulletin creation

## Industry Coordination

Security ratings of issues included in Android security bulletins and these bulletins match in the most common scenarios but may differ in some cases due to one of the following reasons:

- Consideration of security protections such as SELinux not enforced on some platforms
- Differences in assessment of some specific scenarios that involves local denial of service or privilege escalation vulnerabilities in the high level OS kernel

All Qualcomm products mentioned herein are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other product and brand names may be trademarks or registered trademarks of their respective owners.

This technical data may be subject to U.S. and international export, re-export, or transfer (“export”) laws. Diversion contrary to U.S. and international law is strictly prohibited.

Qualcomm Technologies, Inc.  
San Diego, CA 92121  
U.S.A.

© 2022 Qualcomm Technologies, Inc. and/or its subsidiaries. All rights reserved.

Light Dark **Auto**

**Qualcomm**

---

---

**Quick links**

**Company info**

**Stay connected**

Get the latest Qualcomm and industry information delivered to your inbox.

 [Subscribe](#)

[Manage your subscription](#)

---

[Cookie Settings](#)

: [English \(US\)](#)