



Products ▾

Applications ▾

Developer ▾

Support ▾

Company ▾



☰ Documentation

🔍 Search document

Provide Feedback

January 2026 Security Bulletin

Published: 01/05/2026

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 for any questions related to this bulletin.

Table of Contents

Announcements
Acknowledgements
Proprietary Software Issues
Open Source Software Issues
Industry Coordination

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

[Cookie Settings](#) [I Understand](#)

in reporting these issues to us.

	CVE-2025-47334,CVE-2025-47335	conghu
CVE-2025-47394		Xiling G
CVE-2025-47333,CVE-2025-47336,CVE-2025-47337,CVE-2025-47344		heidada
CVE-2025-47369		nicolas

Provide Feedback

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
CVE-2025-47339	High	High	HLOS	Internal
CVE-2025-47343	High	High	Video	Internal
CVE-2025-47345	High	High	Automotive Platform	Internal
CVE-2025-47346	High	High	HLOS	Internal
CVE-2025-47348	High	High	HLOS	Internal
CVE-2025-47356	High	High	Video	Internal
CVE-2025-47380	High	High	Camera	Internal
CVE-2025-47393	High	High	Automotive Linux OS	Internal
CVE-2025-47395	High	Medium	WLAN Firmware	Internal

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

P session.

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	2025/07/07
Affected Chipsets*	AR8035, AR9380, CSR8811, FastConnect 6200, FastConnect 6700, FastConnect 6900, Fa

Provide Feedback

CVE-2025-47343

CVE ID	CVE-2025-47343
Title	Untrusted Pointer Dereference in Video
Description	Memory corruption while processing a video session to set video parameters.
Technology Area	Video
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	2025/07/07
Affected Chipsets*	Cologne, FastConnect 6700, FastConnect 6900, FastConnect 7800, QCA0000, QCM5430,

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

Automotive Platform

ing license data.

ption

Security Rating	High
CVSS Rating	High
CVSS Score	8.4
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/H/I:H/A:N
Date Reported	Internal
Customer Notified Date	2025/07/07
Affected Chipsets*	AR8035, FastConnect 6200, FastConnect 6700, FastConnect 6900, FastConnect 7800, QA

Provide Feedback

CVE-2025-47346

CVE ID	CVE-2025-47346
Title	Out-of-bounds Write in HLOS
Description	Memory corruption while processing a secure logging command in the trusted application
Technology Area	HLOS
Vulnerability Type	CWE-787: Out-of-bounds Write
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	2025/07/07

00, FastConnect 6900, FastConnect 7800, QA

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

credential operations in the trusted applicatic

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	2025/07/07
Affected Chipsets*	AQT1000, AR8035, CSRA6620, CSRA6640, FastConnect 6200, FastConnect 6700, FastCor

Provide Feedback

CVE-2025-47356

CVE ID	CVE-2025-47356
Title	Double Free in Video
Description	Memory Corruption when multiple threads concurrently access and modify shared resource
Technology Area	Video
Vulnerability Type	CWE-415 Double 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

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

00, QCA0000, SC8380XP, WCD9378C, WCD9

LS in sensors.

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	2025/10/06
Affected Chipsets*	FastConnect 7800, QCC2072, WCD9378C, WSA8840, WSA8845, WSA8845H, X2000077, >

Provide Feedback

CVE-2025-47393

CVE ID	CVE-2025-47393
Title	Improper Validation of Array Index in Automotive Linux OS
Description	Memory corruption when accessing resources in kernel driver.
Technology Area	Automotive Linux OS
Vulnerability Type	CWE-129 Improper Validation of Array Index
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

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

/1H, QAMSRV1M, QCA6595, QCA6698AQ, Q

ment frame with a Vendor Specific Informatio

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	2025/10/06
Affected Chipsets*	WCN7861

Provide Feedback

*The list of affected chipsets may not be complete. For latest information, device OEMs can contact QTI directly at 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
				07/06/2025
				07/02/2025
				Internal
				Customer notified and encouraged to patch
				Date Reported
				09/22/2024

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

				Date Reported
CVE-2025-47331	Medium	Medium	Video	10/04/2024
CVE-2025-47332	Medium	Medium	Camera Driver	02/16/2025
CVE-2025-47333	Medium	Medium	HLOS	02/18/2025
CVE-2025-47334	Medium	Medium	Camera Driver	02/16/2025
CVE-2025-47335	Medium	Medium	Camera Driver	02/16/2025
CVE-2025-47336	Medium	Medium	Camera Driver	02/14/2025
CVE-2025-47337	Medium	Medium	Camera Driver	02/11/2025
CVE-2025-47344	Medium	Medium	Camera Driver	02/21/2025
CVE-2025-47369	Medium	Medium	Computer Vision	09/15/2023

CVE-2025-47388

CVE ID	CVE-2025-47388
Title	Buffer Copy without Checking Size of Input in DSP Service
Description	Memory corruption while passing pages to DSP with an unaligned starting address.
Technology Area	DSP Service
Vulnerability Type	CWE-120 Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow')
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	2025/07/06

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

connect 6900, FastConnect 7800, QCS610, QM
[/vendor/qcom/opensource/dsp-kernel/-/comm](#)

DSP Service	
Description	Memory corruption when copying overlapping buffers during memory operations due to in
Technology Area	DSP Service
Vulnerability Type	CWE-120 Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow')
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	2025/07/02
Customer Notified Date	2025/10/06
Affected Chipsets*	FastConnect 6200, FastConnect 6700, FastConnect 6900, FastConnect 7800, QCS610, QM
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/qcom/opensource/dsp-kernel/-/comr

Provide Feedback

CVE-2025-47396

CVE ID	CVE-2025-47396
Title	Double Free in Graphics
Description	Memory corruption occurs when a secure application is launched on a device with insuffic
Technology Area	Graphics
Vulnerability Type	CWE-415 Double Free
Access Vector	Local
Security Rating	High

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

H

connect 6900, FastConnect 7800, QCS610, QM

CVE-2025-47330

CVE ID	CVE-2025-47330
Title	Buffer Over-read in Video
Description	Transient DOS while parsing video packets received from the video firmware.
Technology Area	Video
Vulnerability Type	CWE-126 Buffer Over-read
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	2024/09/22
Customer Notified Date	2025/07/07
Affected Chipsets*	AR8031, AR8035, CSRA6620, CSRA6640, C-V2X 9150, FastConnect 6200, FastConnect 67
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/kernel/msm-5.15/-/commit/91ac2abd7ede6e837746

Provide Feedback

CVE-2025-47331

CVE ID	CVE-2025-47331
Title	Buffer Over-read in Video

firmware event.

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

Date Reported	2024/10/04
Customer Notified Date	2025/07/07
Affected Chipsets*	AR8031, AR8035, CSR8811, CSRA6620, CSRA6640, FastConnect 6200, FastConnect 6700
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/kernel/msm-5.15/-/commit/b987bc28efb34989add61

Provide Feedback

CVE-2025-47332

CVE ID	CVE-2025-47332
Title	Time-of-check Time-of-use (TOCTOU) Race Condition in Camera Driver
Description	Memory corruption while processing a config call from userspace.
Technology Area	Camera Driver
Vulnerability Type	CWE-367 Time-of-check Time-of-use (TOCTOU) Race Condition
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.7
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Date Reported	2025/02/16
Customer Notified Date	2025/07/07
Affected Chipsets*	FastConnect 6200, FastConnect 6700, FastConnect 6900, FastConnect 7800, QCA6698AL
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/camera-kernel/-/commit

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

opping operations in the cryptographic driver.

Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.6
CVSS String	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L
Date Reported	2025/02/18
Customer Notified Date	2025/07/07
Affected Chipsets*	AQT1000, AR8031, AR8035, CSRA6620, CSRA6640, CSRB31024, C-V2X 9150, FastConnect
Patch**	<ul style="list-style-type: none"> https://git.codelinear.org/clo/la/platform/vendor/qcom/opensource/securemsm-kernel/-/commit/6336304b4e597b8e92d2 https://git.codelinear.org/clo/la/kernel/msm-5.10/-/commit/6336304b4e597b8e92d2

Provide Feedback

CVE-2025-47334

CVE ID	CVE-2025-47334
Title	Buffer Copy Without Checking Size of Input in Camera Driver
Description	Memory corruption while processing shared command buffer packet between camera user
Technology Area	Camera Driver
Vulnerability Type	CWE-120 Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow')
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.7
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

FastConnect 6700, FastConnect 6900, FastConnect

[/vendor/opensource/camera-kernel/-/commit/6336304b4e597b8e92d2](#)
[/vendor/opensource/camera-kernel/-/commit/6336304b4e597b8e92d2](#)

Title	Buffer Copy Without Checking Size of Input in Camera Driver
Description	Memory corruption while parsing clock configuration data for a specific hardware type.
Technology Area	Camera Driver
Vulnerability Type	CWE-120 Buffer Copy Without Checking Size of Input ('Classic Buffer Overflow')
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.7
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Date Reported	2025/02/16
Customer Notified Date	2025/07/07
Affected Chipsets*	FastConnect 6700, FastConnect 6900, FastConnect 7800, QCA6698AQ, QCM5430, QCM6
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/camera-kernel/-/commit

Provide Feedback

CVE-2025-47336

CVE ID	CVE-2025-47336
Title	Use After Free in Camera Driver
Description	Memory corruption while performing sensor register read operations.
Technology Area	Camera Driver
Vulnerability Type	CWE-416 Use After Free
Access Vector	Local

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

:H

750, SM8750P, WCD9378, WCD9395, WCN77

[/vendor/opensource/camera-kernel/-/commit](#)

CVE-2025-47337

CVE ID	CVE-2025-47337
Title	Use After Free in Camera Driver
Description	Memory corruption while accessing a synchronization object during concurrent operations
Technology Area	Camera Driver
Vulnerability Type	CWE-416 Use After Free
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.7
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Date Reported	2025/02/11
Customer Notified Date	2025/07/07
Affected Chipsets*	FastConnect 6700, FastConnect 6900, FastConnect 7800, QCA6391, QCA6698AQ, QCA66
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/camera-kernel/-/commit https://git.codelinaro.org/clo/le/platform/vendor/opensource/camera-kernel/-/commit

Provide Feedback

CVE-2025-47344

CVE ID	CVE-2025-47344
Title	Time-of-check Time-of-use (TOCTOU) Race Condition in Camera Driver
Description	Memory corruption while accessing a synchronization object during concurrent operations.
Technology Area	Camera Driver
Vulnerability Type	CWE-362 (TOCTOU) Race Condition
Access Vector	Local
Security Rating	Medium
CVSS Rating	Medium
CVSS Score	6.7
CVSS String	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Date Reported	2025/02/11
Customer Notified Date	2025/07/07
Affected Chipsets*	FastConnect 6700, FastConnect 6900, FastConnect 7800, QCA6391, QCA6698AQ, QCA66
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/camera-kernel/-/commit https://git.codelinaro.org/clo/le/platform/vendor/opensource/camera-kernel/-/commit

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

Date Reported	2025/02/21
Customer Notified Date	2025/07/07
Affected Chipsets*	CSRA6620, CSRA6640, FastConnect 6200, FastConnect 6700, FastConnect 6900, FastCor
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/camera-kernel/-/commit

Provide Feedback

CVE-2025-47369

CVE ID	CVE-2025-47369
Title	Information Exposure in Computer Vision
Description	Information disclosure when a weak hashed value is returned to userland code in response
Technology Area	Computer Vision
Vulnerability Type	CWE-200 Information Exposure
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:H/I:N/A:N
Date Reported	2023/09/15
Customer Notified Date	2025/08/04
Affected Chipsets*	AR8035, CSRA6620, CSRA6640, FastConnect 6200, FastConnect 6700, FastConnect 6800
Patch**	<ul style="list-style-type: none"> https://git.codelinaro.org/clo/la/platform/vendor/opensource/eva-kernel/-/commit/b2f

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

formation, device OEMs can contact

and these bulletins match in the most
the following reasons:

pt 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.

Provide Feedback

Light Dark **Auto**



Qualcomm relentlessly innovates to deliver intelligent computing everywhere, helping the world tackle some of its most important challenges. Our leading-edge AI, high performance, low-power computing, and unrivaled connectivity deliver proven solutions that transform major industries. At Qualcomm, we are engineering human progress.



This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.

d
 Qualcomm and industry information delivered to your
 e
 pscription

Email Subscriptions

Provide Feedback

[Terms of Use](#) [Privacy](#) [Cookie Policy](#) [Accessibility Statement](#) [Cookie Settings](#)

Language: English (US)

© Qualcomm Technologies, Inc. and/or its affiliated companies.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries. Qualcomm patented technologies are licensed by Qualcomm Incorporated.

Note: Certain services and materials may require you to accept additional terms and conditions before accessing or using those items.

References to "Qualcomm" may mean Qualcomm Incorporated, or subsidiaries or business units within the Qualcomm corporate structure, as applicable.

Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Materials that are as of a specific date, including but not limited to press releases, presentations, blog posts and webcasts, may have been superseded by subsequent events or disclosures.

Nothing in these materials is an offer to sell or license any of the services or materials referenced herein.

This website processes personal data through our and third parties' online tracking technologies, including analytics and advertising cookies. To learn more about how we and our affiliates within the Qualcomm Group may use your personal data and cookies, please review the Privacy Policy published at the bottom of this website and Qualcomm's [Cookie Policy](#). If you don't want to share your website activities, including browsing behavior, with our third-party partners via these tracking technologies, click on "Cookie Settings" below to update your preferences. You can also update your cookie preferences at any time by clicking the [Do Not Sell or Share My Personal Information](#) link at the bottom of this website.