Untrusted Pointer Dereference in Power Optimization Firmware

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-47408
State	PUBLISHED
Assigner	qualcomm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 17:16:21 UTC
Updated	2026-05-06 18:03:00 UTC
Description	Memory corruption when another driver calls an IOCTL with invalid input/output buffer.

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from product-security@qualcomm.com

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000150000 probability, percentile 0.032440000 (date 2026-05-05)

Problem Types: CWE-822 | CWE-119 | CWE-822 CWE-822 Untrusted Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	product-security@qualcomm.com	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qualcomm	Fastconnect 6200	-	All	All	All
Operating System	Qualcomm	Fastconnect 6200 Firmware	-	All	All	All
Hardware	Qualcomm	Fastconnect 6900	-	All	All	All
Operating System	Qualcomm	Fastconnect 6900 Firmware	-	All	All	All
Hardware	Qualcomm	Fastconnect 7800	-	All	All	All
Operating System	Qualcomm	Fastconnect 7800 Firmware	-	All	All	All
Hardware	Qualcomm	Iqx5121	-	All	All	All
Operating System	Qualcomm	Iqx5121 Firmware	-	All	All	All
Hardware	Qualcomm	Iqx7181	-	All	All	All
Operating System	Qualcomm	Iqx7181 Firmware	-	All	All	All
Hardware	Qualcomm	Qca0000	-	All	All	All
Operating System	Qualcomm	Qca0000 Firmware	-	All	All	All
Hardware	Qualcomm	Sc8380xp	-	All	All	All
Operating System	Qualcomm	Sc8380xp Firmware	-	All	All	All
Hardware	Qualcomm	Sd865 5g	-	All	All	All
Operating System	Qualcomm	Sd865 5g Firmware	-	All	All	All
Hardware	Qualcomm	Sm6250	-	All	All	All
Operating System	Qualcomm	Sm6250 Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 7c Compute	-	All	All	All
Operating System	Qualcomm	Snapdragon 7c Compute Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 7c Gen 2 Compute	-	All	All	All
Operating System	Qualcomm	Snapdragon 7c Gen 2 Compute Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon Xr2 Gen 1	-	All	All	All
Operating System	Qualcomm	Snapdragon Xr2 Gen 1 Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon Xr2 5g	-	All	All	All
Operating System	Qualcomm	Snapdragon Xr2 5g Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9380	-	All	All	All
Operating System	Qualcomm	Wcd9380 Firmware	-	All	All	All

Hardware	Qualcomm	Wcd9385	-	All	All	All
Operating System	Qualcomm	Wcd9385 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8810	-	All	All	All
Operating System	Qualcomm	Wsa8810 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8815	-	All	All	All
Operating System	Qualcomm	Wsa8815 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8840	-	All	All	All
Operating System	Qualcomm	Wsa8840 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8845	-	All	All	All
Hardware	Qualcomm	Wsa8845h	-	All	All	All
Operating System	Qualcomm	Wsa8845h Firmware	-	All	All	All
Operating System	Qualcomm	Wsa8845 Firmware	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6200	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6900	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 7800	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected IQX5121	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected IQX7181	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected QCA0000	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected SC8380XP	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected SD865 5G	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected SM6250	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 7c Compute Platform	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 7c Gen 2 Compute Platform "Rennell Pro"	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon XR2 5G Platform	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon XR2+ Gen 1 Platform	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WCD9380	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WCD9385	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WSA8810	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WSA8815	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WSA8840	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845	Snapdragon Compute, Snapdra
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845H	Snapdragon Compute, Snapdra

References

Reference	Source	Link
docs.qualcomm.com/product/publicresources/securitybulletin/may-2026-bulletin.html	product-security@qualcomm.com	docs.qualcomm.cc
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.