Exposed dangerous function in windows host

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

Summary

CVE	CVE-2026-25266
State	PUBLISHED
Assigner	qualcomm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 17:16:22 UTC
Updated	2026-05-06 18:02:02 UTC
Description	Memory corruption while processing IOCTL command when device is in power-save state.

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.000150000 probability, percentile 0.032180000 (date 2026-05-05)

Problem Types: CWE-749 | CWE-787 | CWE-749 CWE-749: Exposed Dangerous Method or Function

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	product-security@qualcomm.com	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

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	Cologne	-	All	All	All
Operating System	Qualcomm	Cologne 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	Sc8380xp	-	All	All	All
Operating System	Qualcomm	Sc8380xp Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon Ar1 Gen 1	-	All	All	All
Operating System	Qualcomm	Snapdragon Ar1 Gen 1 Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9378c	-	All	All	All
Operating System	Qualcomm	Wcd9378c 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	Wcn7861	-	All	All	All
Operating System	Qualcomm	Wcn7861 Firmware	-	All	All	All
Hardware	Qualcomm	Wcn7880	-	All	All	All
Operating System	Qualcomm	Wcn7880 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8830	-	All	All	All
Operating System	Qualcomm	Wsa8830 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8832	-	All	All	All
Operating System	Qualcomm	Wsa8832 Firmware	-	All	All	All
Hardware	Qualcomm	Wsa8835	-	All	All	All
Operating System	Qualcomm	Wsa8835 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
Hardware	Qualcomm	X2000077	-	All	All	All
Operating System	Qualcomm	X2000077 Firmware	-	All	All	All
Hardware	Qualcomm	X2000086	-	All	All	All
Operating System	Qualcomm	X2000086 Firmware	-	All	All	All
Hardware	Qualcomm	X2000090	-	All	All	All
Operating System	Qualcomm	X2000090 Firmware	-	All	All	All
Hardware	Qualcomm	X2000092	-	All	All	All
Operating System	Qualcomm	X2000092 Firmware	-	All	All	All
Hardware	Qualcomm	X2000094	-	All	All	All
Operating System	Qualcomm	X2000094 Firmware	-	All	All	All
Hardware	Qualcomm	Xg101002	-	All	All	All
Operating System	Qualcomm	Xg101002 Firmware	-	All	All	All
Hardware	Qualcomm	Xg101032	-	All	All	All
Operating System	Qualcomm	Xg101032 Firmware	-	All	All	All
Hardware	Qualcomm	Xg101039	-	All	All	All
Operating System	Qualcomm	Xg101039 Firmware	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Qualcomm Inc.	Snapdragon	affected Cologne	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6900	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 7800	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected SC8380XP	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon AR1 Gen 1 Platform	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WCD9378C	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WCD9380	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WCD9385	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WCN7861	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WCN7880	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WSA8830	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WSA8832	Snapdragon CCW, Snapdragon Compute, Snapdrago

CNA	Qualcomm Inc.	Snapdragon	affected WSA8835	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WSA8840	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845H	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected X2000077	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected X2000086	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected X2000090	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected X2000092	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected X2000094	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected XG101002	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected XG101032	Snapdragon CCW, Snapdragon Compute, Snapdrago
CNA	Qualcomm Inc.	Snapdragon	affected XG101039	Snapdragon CCW, Snapdragon Compute, Snapdrago

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.