



Buffer Over-read in Computer Vision

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2025-47400
State	PUBLISHED
Assigner	qualcomm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 16:16:28 UTC
Updated	2026-04-08 21:05:12 UTC
Description	Cryptographic issue while copying data to a destination buffer without validating its size.

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from product-security@qualcomm.com

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

EPSS: 0.000050000 probability, percentile 0.002060000 (date 2026-04-13)

Problem Types: CWE-126 | CWE-126 CWE-126 Buffer Over-read

Version	Source	Type	Score	Severity	Vector
3.1	product-security@qualcomm.com	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Qualcomm	Pandeiro	-	All	All	All
Operating System	Qualcomm	Pandeiro Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 8 Elite Gen 5	-	All	All	All
Operating System	Qualcomm	Snapdragon 8 Elite Gen 5 Firmware	-	All	All	All
Hardware	Qualcomm	Sw6100	-	All	All	All
Hardware	Qualcomm	Sw6100p	-	All	All	All
Operating System	Qualcomm	Sw6100p Firmware	-	All	All	All
Operating System	Qualcomm	Sw6100 Firmware	-	All	All	All
Hardware	Qualcomm	Themisto	-	All	All	All
Operating System	Qualcomm	Themisto Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9395	-	All	All	All
Operating System	Qualcomm	Wcd9395 Firmware	-	All	All	All
Hardware	Qualcomm	Wcn7860	-	All	All	All
Operating System	Qualcomm	Wcn7860 Firmware	-	All	All	All
Hardware	Qualcomm	Wcn7861	-	All	All	All
Operating System	Qualcomm	Wcn7861 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 Pandeiro	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 8 Elite Gen 5	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected SW6100	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected SW6100P	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected Themisto	Snapdragon Compute, Snapdragon Wearables

CNA	Qualcomm Inc.	Snapdragon	affected Hmem120	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WCD9395	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WCN7860	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WCN7861	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WSA8840	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845	Snapdragon Compute, Snapdragon Wearables
CNA	Qualcomm Inc.	Snapdragon	affected WSA8845H	Snapdragon Compute, Snapdragon Wearables

References

Reference	Source	Link
docs.qualcomm.com/product/publicresources/securitybulletin/april-2026-bulletin...	product-security@qualcomm.com	docs.qualcomm.com
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report