



# Buffer Over-read in Camera

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

## Summary

<b>CVE</b>	CVE-2026-21378
<b>State</b>	PUBLISHED
<b>Assigner</b>	qualcomm
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-06 16:16:30 UTC
<b>Updated</b>	2026-04-08 20:53:42 UTC
<b>Description</b>	Memory Corruption when accessing an output buffer without validating its size during IOCTL processing in a camera senso

## 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:** 0.000130000 probability, percentile 0.019790000 (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	7.8	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

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	Aqt1000	-	All	All	All
Operating System	Qualcomm	Aqt1000 Firmware	-	All	All	All
Hardware	Qualcomm	Cologne	-	All	All	All
Operating System	Qualcomm	Cologne Firmware	-	All	All	All
Hardware	Qualcomm	Fastconnect 6200	-	All	All	All
Operating System	Qualcomm	Fastconnect 6200 Firmware	-	All	All	All
Hardware	Qualcomm	Fastconnect 6700	-	All	All	All
Operating System	Qualcomm	Fastconnect 6700 Firmware	-	All	All	All
Hardware	Qualcomm	Fastconnect 6800	-	All	All	All
Operating System	Qualcomm	Fastconnect 6800 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	Qca0000	-	All	All	All
Operating System	Qualcomm	Qca0000 Firmware	-	All	All	All
Hardware	Qualcomm	Qca6391	-	All	All	All
Operating System	Qualcomm	Qca6391 Firmware	-	All	All	All
Hardware	Qualcomm	Qca6420	-	All	All	All
Operating System	Qualcomm	Qca6420 Firmware	-	All	All	All
Hardware	Qualcomm	Qca6430	-	All	All	All
Operating System	Qualcomm	Qca6430 Firmware	-	All	All	All
Hardware	Qualcomm	Qcm5430	-	All	All	All
Operating System	Qualcomm	Qcm5430 Firmware	-	All	All	All
Hardware	Qualcomm	Qcm6490	-	All	All	All
Operating System	Qualcomm	Qcm6490 Firmware	-	All	All	All
Hardware	Qualcomm	Sc8380xp	-	All	All	All
Operating System	Qualcomm	Sc8380xp Firmware	-	All	All	All
Hardware	Qualcomm	Sm6250	-	All	All	All

Operating System	Qualcomm	Sm6250 Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 460 Mobile Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 460 Mobile Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 662 Mobile Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 662 Mobile Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 7c Gen 3 Compute	-	All	All	All
Operating System	Qualcomm	Snapdragon 7c Gen 3 Compute Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 7c Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 7c Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 7c Gen 2 Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 7c Gen 2 Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 8cx Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 8cx Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 8cx Gen 2 5g Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 8cx Gen 2 5g Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 8cx Gen 3 Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 8cx Gen 3 Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon 8c Compute Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon 8c Compute Platform Firmware	-	All	All	All
Hardware	Qualcomm	Snapdragon Ar1 Gen 1 Platform	-	All	All	All
Operating System	Qualcomm	Snapdragon Ar1 Gen 1 Platform Firmware	-	All	All	All
Hardware	Qualcomm	Video Collaboration Vc3 Platform	-	All	All	All
Operating System	Qualcomm	Video Collaboration Vc3 Platform Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9340	-	All	All	All
Operating System	Qualcomm	Wcd9340 Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9341	-	All	All	All
Operating System	Qualcomm	Wcd9341 Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9370	-	All	All	All
Operating System	Qualcomm	Wcd9370 Firmware	-	All	All	All
Hardware	Qualcomm	Wcd9375	-	All	All	All
Operating System	Qualcomm	Wcd9375 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	Wcn3950	-	All	All	All
Operating System	Qualcomm	Wcn3950 Firmware	-	All	All	All
Hardware	Qualcomm	Wcn3988	-	All	All	All
Operating System	Qualcomm	Wcn3988 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	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

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 AQT1000	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Cologne	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6200	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6700	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6800	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 6900	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected FastConnect 7800	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCA0000	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCA6391	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCA6420	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCA6430	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCM5430	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected QCM6490	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Qualcomm Video Collaboration VC3 Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected SC8380XP	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected SM6250	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 460 Mobile Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 662 Mobile Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 7c Compute Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 7c Gen 2 Compute Platform "Rennell Pro"	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 7c+ Gen 3 Compute	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 8c Compute Platform "Poipu Lite"	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 8cx Compute Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 8cx Gen 2 5G Compute Platform "Poipu Pro"	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon 8cx Gen 3 Compute Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected Snapdragon AR1 Gen 1 Platform	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected WCD9340	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected WCD9341	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected WCD9370	Snapdragon Compute, Snapd
CNA	Qualcomm Inc.	Snapdragon	affected WCD9375	Snapdragon Compute, Snapd

CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WCD9378C	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WCD9380	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WCD9385	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WCN3950	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WCN3988	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8810	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8815	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8830	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8832	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8835	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8840	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8845	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected WSA8845H	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected X2000077	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected X2000086	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected X2000090	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected X2000092	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected X2000094	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected XG101002	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected XG101032	Snapdragon Compute, Snap
CNA	<a href="#">Qualcomm Inc.</a>	<a href="#">Snapdragon</a>	affected XG101039	Snapdragon Compute, Snap

## References

Reference	Source	Link
<a href="https://docs.qualcomm.com/product/publicresources/securitybulletin/april-2026-bulletin...">docs.qualcomm.com/product/publicresources/securitybulletin/april-2026-bulletin...</a>	product-security@qualcomm.com	<a href="https://docs.qualcomm.com">docs.qualcomm.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)