

CVE-2023-33106

Qualcomm Multiple Chipsets Use of Out-of-Range Pointer Offset Vulnerability

CISA KEV since Dec 5, 2023

Actively exploited

Memory corruption while submitting a large list of sync points in an AUX command to the IOCTL_KGSL_GPU_AUX_COMMAND.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.008 55.7th percentile · FIRST	CISA DEADLINE Dec 26, 2023 KEV since 2023 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.008 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply remediations or mitigations per vendor instructions or discontinue use of the product if remediation or mitigations are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions · 298 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ar8035 firmware	—	no fixed version listed	NVD
csra6620 firmware	—	no fixed version listed	NVD
csra6640 firmware	—	no fixed version listed	NVD
fastconnect 6200 firmware	—	no fixed version listed	NVD
fastconnect 6700 firmware	—	no fixed version listed	NVD
fastconnect 6800 firmware	—	no fixed version listed	NVD
fastconnect 6900 firmware	—	no fixed version listed	NVD
fastconnect 7800 firmware	—	no fixed version listed	NVD

Sources

Vendor guidance	qualcomm.com/company/product-security/bulletins/december-2023-bulletin	git.codelinearo.org	git.codelinearo.org/clo/la/kernel/msm-4.19/-/commit/1e46e81db6b69aafd5842ce779f07e617680fd58
NVD	nvd.nist.gov/vuln/detail/CVE-2023-33106	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2023-37295	Current data	evulnabile.com/vulnerability-management/cve/CVE-2023-33106

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.