

CVE-2025-27038

Qualcomm Multiple Chipsets Use-After-Free Vulnerability

CISA KEV since Jun 3, 2025

Actively exploited

Memory corruption while rendering graphics using Adreno GPU drivers in Chrome.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.010 63rd percentile · FIRST	CISA DEADLINE Jun 24, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.010 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Please check with specific vendors (OEMs,) for information on patching status.

Basis: CISA KEV required action

Affected and fixed versions · 80 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
ar8031 firmware	—	no fixed version listed	NVD
csra6620 firmware	—	no fixed version listed	NVD
csra6640 firmware	—	no fixed version listed	NVD
fastconnect 7800 firmware	—	no fixed version listed	NVD
qca2066 firmware	—	no fixed version listed	NVD
qca6391 firmware	—	no fixed version listed	NVD
qcm6125 firmware	—	no fixed version listed	NVD
qcm8550 firmware	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-h454-pc9h-rvh2

Additional guidance docs.qualcomm.com/product/publicresources/securitybulletin/june-2025-bulletin.html

NVD nvd.nist.gov/vuln/detail/CVE-2025-27038

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-16700

Current data evulnable.com/vulnerability-management/cve/CVE-2025-27038

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