

CVE-2020-11261

Qualcomm Multiple Chipsets Improper Input Validation Vulnerability

CISA KEV since Dec 1, 2021

Actively exploited

Memory corruption due to improper check to return error when user application requests memory allocation of a huge size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.016 75.7th percentile · FIRST	CISA DEADLINE Jun 1, 2022 KEV since 2021 · 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	0.016 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 updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 790 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
apq8009 firmware	—	no fixed version listed	NVD
apq8009w firmware	—	no fixed version listed	NVD
apq8017 firmware	—	no fixed version listed	NVD
apq8037 firmware	—	no fixed version listed	NVD
apq8053 firmware	—	no fixed version listed	NVD
apq8064au firmware	—	no fixed version listed	NVD
apq8096au firmware	—	no fixed version listed	NVD
aqt1000 firmware	—	no fixed version listed	NVD

Sources

Vendor guidance	qualcomm.com/company/product-security/bulletins/january-2021-bulletin	NVD	nvd.nist.gov/vuln/detail/CVE-2020-11261
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-3615
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-11261		

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