

CVE-2020-0069

Mediatek Multiple Chipsets Insufficient Input Validation Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

In the ioctl handlers of the Mediatek Command Queue driver, there is a possible out of bounds write due to insufficient input sanitization and missing SELinux restrictions. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-147882143 References: M-ALPS04356754

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.014 71.7th percentile · FIRST	CISA DEADLINE May 3, 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	0.014 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 · 49 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
android	—	no fixed version listed	NVD
berkeley-l09 firmware	< 10.0.0.177\ (c10e3r1p4\)	10.0.0.177\ (c10e3r1p4\)	NVD
columbia-al10b firmware	< 10.0.0.178\ (c00e178r1p4\)	10.0.0.178\ (c00e178r1p4\)	NVD
columbia-l29d firmware	< 10.0.0.177\ (c10e4r1p4\)	10.0.0.177\ (c10e4r1p4\)	NVD
	< 10.0.0.177\ (c432e3r1p4\)		
columbia-tl00b firmware	< 10.0.0.178\ (c01e178r1p4\)	10.0.0.178\ (c01e178r1p4\)	NVD
columbia-tl00d firmware	< 10.0.0.178\ (c01e178r1p4\)	10.0.0.178\ (c01e178r1p4\)	NVD
cornell-al00a firmware	< 9.1.0.340\ (c00e333r1p1t8\)	9.1.0.340\ (c00e333r1p1t8\)	NVD
cornell-tl10b firmware	< 9.1.0.340\ (c01e333r1p1t8\)	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xx48-fp29-wh9j

Additional guidance source.android.com/security/bulletin/2020-03-01

NVD nvd.nist.gov/vuln/detail/CVE-2020-0069

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-1576

Current data evulnable.com/vulnerability-management/cve/CVE-2020-0069

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