

CVE-2020-5722

Grandstream Networks UCM6200 Series SQL Injection Vulnerability

CISA KEV since Jan 28, 2022

Actively exploited

Public exploit module (Metasploit)

The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via crafted HTTP request. An attacker can use this vulnerability to execute shell commands as root on versions before 1.0.19.20 or inject HTML in password recovery emails in versions before 1.0.20.17.

EVRS 83 /100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.844 99.7th percentile · FIRST	CISA DEADLINE Jul 28, 2022 KEV since 2022 · 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	0.844 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
ucm6200 firmware	< 1.0.19.20	1.0.19.20	NVD
ucm6200	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-cgpg-723h-vg48	NVD	nvd.nist.gov/vuln/detail/CVE-2020-5722
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-26881
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-5722		

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