



CVE-2020-5722

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-5722
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-23 20:15:00 UTC
Updated	2022-02-10 07:31:00 UTC
Description	The HTTP interface of the Grandstream UCM6200 series is vulnerable to an unauthenticated remote SQL injection via craft

Risk And Classification

EPSS: 0.927350000 probability, percentile 0.997600000 (date 2026-05-05)

CISA KEY: Listed on 2022-01-28; due 2022-07-28; ransomware use Unknown

Problem Types: CWE-89

CISA Known Exploited Vulnerability

Vendor	Grandstream
Product	UCM6200
Name	Grandstream Networks UCM6200 Series SQL Injection Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-5722

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Grandstream	Ucm6200	-	All	All	All
Hardware	Grandstream	Ucm6200	-	All	All	All
Operating System	Grandstream	Ucm6200 Firmware	All	All	All	All
Operating System	Grandstream	Ucm6200 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
UCM6202 1.0.18.13 Remote Command Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Third Party

Grandstream UCM62xx SQL Injection - Research Advisory Tenable®	MISC	www.tenable.com	Thir
Grandstream UCM62xx IP PBX sendPasswordEmail Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report