< CVEs

CVE-2020-5756

HIGH

Information CPEs Plugins

Description

Grandstream GWN7000 firmware version 1.0.9.4 and below allows authenticated remote users to modify the system's crontab via undocumented API. An attacker can use this functionality to execute arbitrary OS commands on the router.

References

https://www.tenable.com/cve/CVE-2020-5756

https://www.tenable.com/security/research/tra-2020-41

Details

Source: MITRE

Published: 2020-07-17

Updated: 2020-07-22

Type: CWE-78

Risk Information

CVSS v2

Base Score: 9

Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C

Impact Score: 10

Exploitability Score: 8

Severity: HIGH

CVSS v3

Base Score: 8.8

Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Impact Score: 5.9

Exploitability Score: 2.8

Severity: HIGH