



CVE-2020-19419

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

Summary

CVE	CVE-2020-19419
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-10 18:15:00 UTC
Updated	2022-10-05 18:28:00 UTC
Description	Incorrect Access Control in Emerson Smart Wireless Gateway 1420 4.6.59 allows remote attackers to obtain sensitive device information.

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Emerson	Smart Wireless Gateway 1420	-	All	All	All
Operating System	Emerson	Smart Wireless Gateway 1420 Firmware	4.6.59	All	All	All

References

Reference	Source	Link	Tags
Emerson Smart Wireless Gateway 1420 4.6.59 Missing Authentication ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party
CWE - CWE-306: Missing Authentication for Critical Function (4.3)	MISC	cve.mitre.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, primary

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)