



CVE-2020-35785

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

Summary

CVE	CVE-2020-35785
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-30 00:15:00 UTC
Updated	2020-12-31 14:40:00 UTC
Description	NETGEAR DGN2200v1 devices before v1.0.0.60 mishandle HTTPd authentication (aka PSV-2020-0363, PSV-2020-0364,

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Dgn2200	v1	All	All	All
Hardware	Netgear	Dgn2200	v1	All	All	All
Operating System	Netgear	Dgn2200 Firmware	All	All	All	All
Operating System	Netgear	Dgn2200 Firmware	All	All	All	All

References

Reference	Source	Link
Security Advisory for Multiple HTTPd Authentication Vulnerabilities on DGN2200v1 Answer NETGEAR Support	MISC	kb.netgear.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#) 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](#)