



CVE-2021-45677

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

Summary

CVE	CVE-2021-45677
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-26 01:15:00 UTC
Updated	2022-01-05 13:01:00 UTC
Description	Certain NETGEAR devices are affected by stored XSS. This affects GS108Tv2 before 5.4.2.36 and GS110TPv2 before 5.4

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Gs108t	v2	All	All	All
Operating System	Netgear	Gs108t Firmware	All	All	All	All
Hardware	Netgear	Gs110tp	v2	All	All	All
Operating System	Netgear	Gs110tp Firmware	All	All	All	All

References

Reference	S
Security Advisory for Stored Cross Site Scripting on Some Smart Managed Pro Switches, PSV-2019-0191 Answer NETGEAR Support	M
CVE Program record	C
NVD vulnerability detail	N

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](#).

Free CVE JSON API cve.report/api

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