



CVE-2021-38702

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

Summary

CVE	CVE-2021-38702
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-17 20:15:00 UTC
Updated	2021-08-25 16:52:00 UTC
Description	Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cyberoamworks	Netgenie C0101b1-20141120-ng11vo	-	All	All	All
Operating System	Cyberoamworks	Netgenie C0101b1-20141120-ng11vo Firmware	All	All	All	All

References

Reference	Source	Link
Cyberoam NetGenie Cross Site Scripting ~ Packet Storm	MISC	packetstormsecurity.com
Full Disclosure: Cyberoam NetGenie (C0101B1-20141120-NG11VO) - Cross Site Scripting (XSS)	FULLDISC	seclists.org
Cyberoam NetGenie for Home Unified Threat Management CyberoamWorks.com	MISC	www.cyberoamworks.com
Full Disclosure: Cyberoam NetGenie (C0101B1-20141120-NG11VO) - Cross Site Scripting (XSS)	MISC	seclists.org
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.

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](#) 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