Cyberoam NetGenie (C0101B1-20141120-NG11VO) - Cross Site Scripting (XSS)

From: Gionathan Reale via Fulldisclosure <fulldisclosure () seclists org>
Date: Sun, 15 Aug 2021 10:10:17 +0200 (CEST)

```
# Title: Cyberoam NetGenie (C0101B1-20141120-NG11VO) - Reflected Cross Site Scripting (XSS)# Date: 14.08.2021 #
Credit:
Gionathan "John" Reale # Firmware Version: C0101B1-20141120-NG11VO#
CVE-2021-
38702#################################################################################################################
#################
 DESCRIPTION:
Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks.
POC:

After connecting to the network via the NetGenie router a page is displayed suggesting a redirect, within the redirect
parameter it is possible to execute reflected Cross Site Scripting, the component affected is "hxxp:/URL/tweb/ft.php?
u="




_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **Cyberoam NetGenie (C0101B1-20141120-NG11VO) - Cross Site Scripting (XSS)** ***Gionathan Reale via Fulldisclosure (Aug 16)***

Site Search

Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License