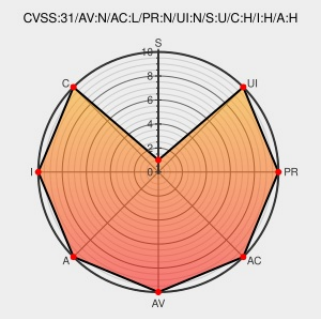
CVE-2021-27708

Published on: 04/14/2021 12:00:00 AM UTC

Last Modified on: 04/21/2021 03:38:00 PM UTC

CVE-2021-27708

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of A720r from Totolink contain the following vulnerability:

Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS.

CVE-2021-27708 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
totolink vulnerability - HackMD		MISC hackmd.io/mDqIBvoxSRCZrZiZifQCbw

totolink vulnerability - HackMD	hackmd.io text/html	MISC hackmd.io/mDgIBv0xSPC2r2I2jIQGhw
totolink vulnerability - HackMD	hackmd.io text/html	MISC hackmd.io/7FtB06f-SJ-SCfkMYcXYxA

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Totolink	A720r	-	All	All	All
Operating System	Totolink	A720r Firmware	4.1.5cu.470_b20200911	All	All	All
Hardware	Totolink	X5000r	-	All	All	All
Operating System	Totolink	X5000r Firmware	9.1.0u.6118_b20201102	All	All	All

cpe:2.3:h:totolink:a720r:-:*:*:*:*:*:*:*:

cpe:2.3:o:totolink:a720r_firmware:4.1.5cu.470_b20200911:*:*:*:*:*:*:*:

cpe:2.3:h:totolink:x5000r:-:*:*:*:*:*:*:*:

cpe:2.3:o:totolink:x5000r_firmware:9.1.0u.6118_b20201102:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-27708 : Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102 allows remote att… twitter.com/i/web/status/1…	2021-04-14 15:42:49
/r/netcve	CVE-2021-27708	2021-04-14 15:46:37

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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