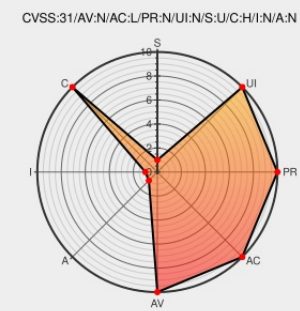
CVE-2021-45735

Published on: Not Yet Published

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-45735

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



Certain versions of X5000r from Totolink contain the following vulnerability:

TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to use the HTTP protocol for authentication into the admin interface, allowing attackers to intercept user credentials via packet capture software.

CVE-2021-45735 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
my_vuln/12.md at main · pjqwudi/my_vuln · GitHub	github.com text/html	MISC github.com/pjqwudi/my_vuln/blob/main/totolink/vuln_12/12.md

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	X5000r	-	All	All	All
Operating System	Totolink	X5000r Firmware	9.1.0u.6118_b20201102	All	All	All

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-2021-45735 : TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to use the HTTP protocol for authentication… twitter.com/i/web/status/1…	2022-02-04 02:20:10

← Previous ID

Next ID→