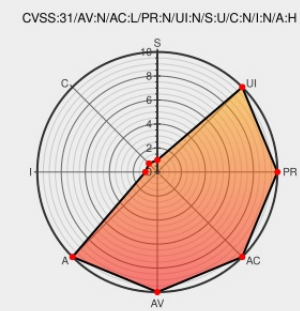
CVE-2023-34669

Published on: Not Yet Published

Last Modified on: 07/26/2023 12:33:00 AM UTC

CVE-2023-34669

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



Certain versions of Cp300 from Totolink contain the following vulnerability:

TOTOLINK CP300+ V5.2cu.7594 contains a Denial of Service vulnerability in function RebootSystem of the file lib/cste_modules/system which can reboot the system.

CVE-2023-34669 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	NONE	NONE	HIGH

CVE References

Description	Tags	Link
Notion – The all-in-one workspace for your notes, tasks, wikis, and databases.	w3b5h3ll.notion.site text/html	MISC w3b5h3ll.notion.site/w3b5h3ll/TOTOLINK-CP300-c96d775881f0476b9ef465dba9c6d9b8

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	Cp300	-	All	All	All
Operating System	Totolink	Cp300 Firmware	5.2cu.7594	All	All	All

cpe:2.3:h:totolink:cp300\+:-:*:*:*:*:*:*:*:

cpe:2.3:o:totolink:cp300\+_firmware:5.2cu.7594:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→