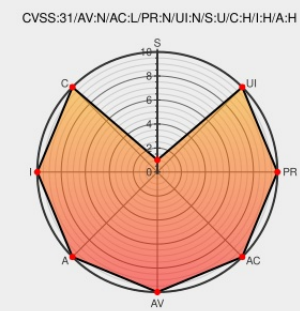
CVE-2023-36952

Published on: Not Yet Published

Last Modified on: 10/19/2023 11:10:00 AM UTC

CVE-2023-36952

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



Certain versions of Cp300 from Totolink contain the following vulnerability:

TOTOLINK CP300+ V5.2cu.7594_B20200910 was discovered to contain a stack overflow via the pingIp parameter in the function setDiagnosisCfg.

CVE-2023-36952 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

CVE References

Description	Tags	Link
Infomation	github.com text/plain	MISC github.com/Archerber/bug_submit/blob/main/TOTOLINK/CP300%2B_1.md

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_b20200910	All	All	All

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

cpe:2.3:o:totolink:cp300\+_firmware:5.2cu.7594_b20200910:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→