

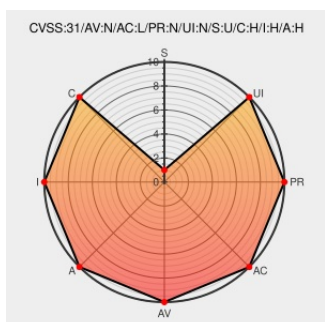


CVE-2023-24138

Published on: Not Yet Published

Last Modified on: 02/10/2023 01:35:00 PM UTC

CVE-2023-24138

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **Ca300-poe** from **Totolink** contain the following vulnerability:

TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the `host_time` parameter in the `NTPSyncWithHost` function.

CVE-2023-24138 has been assigned by [M](#) 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
CVE-vulns/NTPSyncWithHost.md at main · Double-q1015/CVE-vulns · GitHub	github.com text/html	MISC github.com/Double-q1015/CVE-vulns/blob/main/totolink_ca300-poe/NTPSyncWithHost/NTPSyncWithHost.md

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

Exploit/POC from Github

TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the host_time parameter ...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Totolink	Ca300-poe	-	All	All	All
Operating System	Totolink	Ca300-poe Firmware	6.2c.884	All	All	All
cpe:2.3:h:totolink:ca300-poe:-:*:*:*:*:*:						
cpe:2.3:o:totolink:ca300-poe_firmware:6.2c.884:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-24138 : TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the h... twitter.com/i/web/status/1...	2023-02-03 16:09:58
 /r/netcve	CVE-2023-24138	2023-02-03 17:39:24

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)