



CVE-2023-24159

Published on: Not Yet Published

Last Modified on: 02/22/2023 04:33:00 PM UTC

CVE-2023-24159

[Source: Mitre](#)

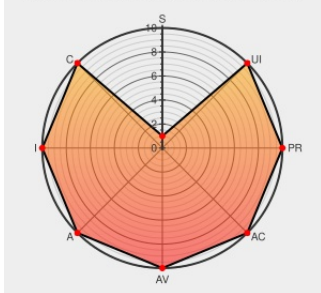
[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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 admpass parameter in the setPasswordCfg function.

CVE-2023-24159 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

VulnerabilityProjectRecords/setPasswordCfg_admpass.md
at main · iceyjchen/VulnerabilityProjectRecords · GitHub

[github.com](#)

[text/html](#)

MISC

github.com/iceyjchen/VulnerabilityProjectRecords/blob/main/setPasswordCfg_admpass.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 admpass parameter in...

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-2023-24159 : TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command injection vulnerability via the a... twitter.com/i/web/status/1...	2023-02-14 15:05:38
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-24159 TOTOLINK CA300-PoE V6.2c.884 was discovered to contain a command... twitter.com/i/web/status/1...	2023-02-14 15:56:01
/r/netcve	CVE-2023-24159	2023-02-14 16:38:32