



CVE-2023-40042

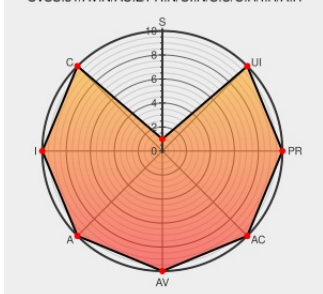
Published on: Not Yet Published

Last Modified on: 08/11/2023 11:37:00 PM UTC

CVE-2023-40042

[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 **T10 V2** from **Totolink** contain the following vulnerability:

TOTOLINK T10_v2 5.9c.5061_B20200511 has a stack-based buffer overflow in setStaticDhcpConfig in /lib/cste_modules/lan.so. Attackers can send crafted data in an MQTT packet, via the comment parameter, to control the return address and execute code.

CVE-2023-40042 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
TOTOLINK全球领先的无线路由设备,无线中继器研发制造厂商	www.totolink.cn text/html	T MISC www.totolink.cn
Information	github.com text/plain	MISC github.com/Korey0sh1/loT_vuln/blob/main/TOTOLINK/T10_V2/setStaticDhcpConfig.md
No Description Provided	www.totolink.net text/html	T MISC www.totolink.net/home/menu/detail/menu_listtpl/download/id/172/ids/36.html

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	T10 V2	-	All	All	All
Operating System	Totolink	T10 V2 Firmware	5.9c.5061_b20200511	All	All	All
cpe:2.3:h:totolink:t10_v2:-:*****:						
cpe:2.3:o:totolink:t10_v2_firmware:5.9c.5061_b20200511:*****:						

No vendor comments have been submitted for this CVE

[← 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](#)