VDB-354128 · CVE-2026-5103 · EUVD-2026-17053

TOTOLINK A3300R 17.0.0CU.557_B20221024 /CGI-BIN/CSTECGI.CGI SETUPNPCFG ENABLE COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	4.02

Summary

A vulnerability described as critical has been identified in Totolink A3300R 17.0.0cu.557_b20221024. Impacted is the function `setUPnPCfg` of the file */cgi-bin/cstecgi.cgi*. Such manipulation of the argument *enable* leads to command injection. This vulnerability is listed as CVE-2026-5103. The attack may be performed from remote. In addition, an exploit is available.

Details

A vulnerability was found in Totolink A3300R 17.0.0cu.557_b20221024 and classified as critical. Affected by this issue is the function `setUPnPCfg` of the file */cgi-bin/cstecgi.cgi*. The manipulation of the argument `enable` with an unknown input leads to a command injection vulnerability. Using CWE to declare the problem leads to CWE-77. The product constructs all or part of a command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended command when it is sent to a downstream component. Impacted is confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is handled as CVE-2026-5103. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1202.

The exploit is available at github.com. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-17053). See VDB-348052, VDB-349642, VDB-352046 and VDB-353863 for similar entries.

Product

Vendor

- Totolink

Name

- A3300R

Version

- 17.0.0cu.557_b20221024

License

- commercial

Website

- Vendor: https://www.totolink.net/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Command injection
CWE: CWE-77 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

03/29/2026		Advisory disclosed
03/29/2026	+0 days	VulDB entry created
03/30/2026	+1 days	VulDB entry last update

Sources

Vendor: totolink.net

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5103 (🔒)
GCVE (CVE): GCVE-0-2026-5103
GCVE (VulDB): GCVE-100-354128
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/29/2026 07:56 PM
Updated: 03/30/2026 05:17 AM
Changes: 03/29/2026 07:56 PM (56), 03/30/2026 05:17 AM (1)
Complete: 🔍
Submitter: LvHW
Cache ID: 20:C9C:179

Submit

Accepted

- Submit #779140: Totolink A3300R 17.0.0cu.557_b20221024 Command Injection (by LvHW)

Discussion

No comments yet. Languages: en.

Please log in to comment.