VDB-354130 · CVE-2026-5105 · GCVE-100-354130

TOTOLINK A3300R 17.0.0CU.557_B20221024 PARAMETER /CGI-BIN/CSTECGI.CGI SETVPNPASSCFG PPTPPASSTHRU COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	3.14

Summary

A vulnerability classified as critical was found in Totolink A3300R 17.0.0cu.557_b20221024. The impacted element is the function `setVpnPassCfg` of the file */cgi-bin/cstecgi.cgi* of the component *Parameter Handler*. Executing a manipulation of the argument *pptpPassThru* can lead to command injection. This vulnerability is registered as CVE-2026-5105. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability was found in Totolink A3300R 17.0.0cu.557_b20221024. It has been declared as critical. This vulnerability affects the function `setVpnPassCfg` of the file */cgi-bin/cstecgi.cgi* of the component *Parameter Handler*. The manipulation of the argument `pptpPassThru` with an unknown input leads to a command injection vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability was named CVE-2026-5105. The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known. This vulnerability is assigned to T1202 by the MITRE ATT&CK project.

It is possible to download the exploit 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.

Similar entries are available at VDB-348052, VDB-349642, VDB-352046 and VDB-353863.

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
03/29/2026	+0 days	VulDB entry last update

Sources

Vendor: totolink.net

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5105 (🔒)
GCVE (CVE): GCVE-0-2026-5105
GCVE (VulDB): GCVE-100-354130
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/29/2026 07:56 PM
Changes: 03/29/2026 07:56 PM (57)
Complete: 🔍
Submitter: LvHW
Cache ID: 145:F63:179

Submit

Accepted

- Submit #779143: Totolink A3300R 17.0.0cu.557_b20221024 Command Injection (by LvHW)

Discussion

No comments yet. Languages: en.

Please log in to comment.