



VDB-354127 · CVE-2026-5102 · GCVE-100-354127

TOTOLINK A3300R 17.0.0CU.557_B20221024 PARAMETER /CGI-BIN/CSTECGI.CGI SETSMARTQOSCFG QOS_UP_BW COMMAND INJECTION

Summary

A vulnerability marked as [critical](#) has been reported in [Totolink A3300R 17.0.0cu.557_b20221024](#). This issue affects the function `setSmartQosCfg` of the file `/cgi-bin/cstecgi.cgi` of the component *Parameter Handler*. This manipulation of the argument `qos_up_bw` causes command injection. This vulnerability is tracked as [CVE-2026-5102](#). The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability has been found in [Totolink A3300R 17.0.0cu.557_b20221024](#) and classified as [critical](#). Affected by this vulnerability is the function `setSmartQosCfg` of the file `/cgi-bin/cstecgi.cgi` of the component *Parameter Handler*. The manipulation of the argument `qos_up_bw` 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.

It is possible to read the advisory at [github.com](#). This vulnerability is known as [CVE-2026-5102](#). The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. The attack technique deployed by this issue is [T1202](#) according to MITRE ATT&CK.

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.

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

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 6.3

VuIDB Meta Temp Score: 5.7

VuIDB Base Score: 6.3

VuIDB Temp Score: 5.7

VuIDB Vector: 

VuIDB 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](https://www.totolink.net)

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5102](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5102](#)

GCVE (VulDB): [GCVE-100-354127](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 03/29/2026 07:56 PM

Changes: 03/29/2026 07:56 PM (57)

Complete: 🔍

Submitter: [LtzHuster2](#)

Cache ID: 68:B14:179

Submit

Accepted

- [Submit #779129](#): Totolink A3300R 17.0.0cu.557_b20221024 Command Injection (by LtzHuster2)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)