



VDB-356377 · CVE-2026-5851 · GCVE-100-356377

TOTOLINK A7100RU 7.4CU.2313_B20191024 CGI /CGI-BIN/CSTECGI.CGI SETUPNPCFG ENABLE OS COMMAND INJECTION

CVSS Meta Temp Score ⓘ

8.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.93-

Summary

A vulnerability was found in [Totolink A7100RU 7.4cu.2313_b20191024](#). It has been rated as **critical**. Affected is the function `setUPnPcFg` of the file `/cgi-bin/csteccgi.cgi` of the component *CGI Handler*. This manipulation of the argument `enable` causes os command injection. This vulnerability is tracked as [CVE-2026-5851](#). The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability has been found in [Totolink A7100RU 7.4cu.2313_b20191024](#) and classified as critical. Affected by this vulnerability is the function `setUPnPcFg` of the file `/cgi-bin/csteccgi.cgi` of the component *CGI Handler*. The manipulation of the argument `enable` with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is [CWE-78](#). The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at [github.com](#). This vulnerability is known as [CVE-2026-5851](#). The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique [T1202](#) for this issue.

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

- [A7100RU](#)

Version

- [7.4cu.2313_b20191024](#)

License

- [commercial](#)

Website

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

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 9.8

VuIDB Meta Temp Score: 8.9

VuIDB Base Score: 9.8

VuIDB Temp Score: 8.9

VuIDB Vector: 

VuIDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Os command injection

CWE: [CWE-78](#) / [CWE-77](#) / [CWE-74](#)

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

- 04/08/2026 █ Advisory disclosed
- 04/08/2026 █ +0 days VulDB entry created
- 04/08/2026 █ +0 days VulDB entry last update

Sources

Vendor: totolink.net

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5851](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5851](#)

GCVE (VulDB): [GCVE-100-356377](#)

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

Entry

Created: 04/08/2026 09:25 PM

Changes: 04/08/2026 09:25 PM (57)

Complete: 🔍

Submitter: [LtzHust2](#)

Cache ID: 104:DB8:179

Submit

Accepted

- [Submit #791271](#): Totolink A7100RU 7.4cu.2313_b20191024 Command Injection (by LtzHust2)

Discussion

No comments yet. Languages: en.

Please log in to comment.