



VDB-356602 · CVE-2026-6026 · GCVE-100-356602

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

CVSS Meta Temp Score

8.9

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.17-

## Summary

A vulnerability categorized as **critical** has been discovered in **Totolink A7100RU 7.4cu.2313\_b20191024**. This issue affects the function `setPortalConfWeChat` of the file `/cgi-bin/cstecgi.cgi` of the component *CGI Handler*. Executing a manipulation of the argument `enable` can lead to os command injection. This vulnerability is tracked as **CVE-2026-6026**. The attack can be launched remotely. Moreover, an exploit is present.

## Details

A vulnerability has been found in **Totolink A7100RU 7.4cu.2313\_b20191024** and classified as **critical**. This vulnerability affects the function `setPortalConfWeChat` of the file `/cgi-bin/cstecgi.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 available at [github.com](https://github.com). This vulnerability was named **CVE-2026-6026**. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. 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](https://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

VulDB Vector: 

VulDB Reliability: 

## CVSSv3

VulDB Meta Base Score: 9.8

VulDB Meta Temp Score: 8.9

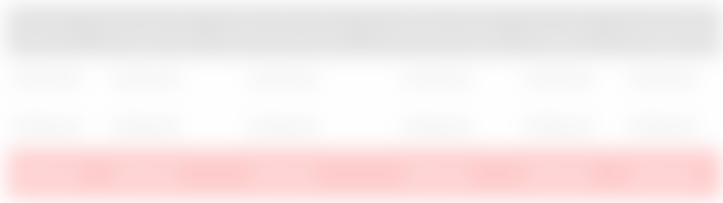
VulDB Base Score: 9.8

VulDB Temp Score: 8.9

VulDB Vector: 

VulDB 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

04/09/2026	█		Advisory disclosed
04/09/2026	█	+0 days	VulDB entry created
04/09/2026	█	+0 days	VulDB entry last update

## Sources

**Vendor:** [totolink.net](https://totolink.net)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-6026](#) (🗝️)

**GCVE (CVE):** [GCVE-0-2026-6026](#)

**GCVE (VulDB):** [GCVE-100-356602](#)

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

## Entry

**Created:** 04/09/2026 06:00 PM

**Changes:** 04/09/2026 06:00 PM (57)

**Complete:** 🔍

**Submitter:** [LtzHust](#)

**Cache ID:** 172:F45:179

## Submit

**Accepted**

- [Submit #792047](#): Totolink A7100RU 7.4cu.2313\_b20191024 Command Injection (by LtzHust)

## Discussion

No comments yet. Languages: en.

Please log in to comment.