



VDB-355516 · CVE-2026-5689 · GCVE-100-355516

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

CVSS Meta Temp Score ⓘ

6.6

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.76-

## Summary

A vulnerability classified as **critical** was found in [Totolink A7100RU 7.4cu.2313\\_b20191024](#). The impacted element is the function `setNtpCfg` of the file `/cgi-bin/cstecgi.cgi`. Executing a manipulation of the argument `tz` can lead to os command injection. This vulnerability is handled as [CVE-2026-5689](#). The attack can be executed remotely. Additionally, an exploit exists.

## Details

A vulnerability was found in [Totolink A7100RU 7.4cu.2313\\_b20191024](#). It has been declared as critical. This vulnerability affects the function `setNtpCfg` of the file `/cgi-bin/cstecgi.cgi`. The manipulation of the argument `tz` 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 for download at [github.com](#). This vulnerability was named [CVE-2026-5689](#). 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. The MITRE ATT&CK project declares the attack technique as [T1202](#).

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.

Entries connected to this vulnerability are available at [VDB-354245](#), [VDB-354246](#), [VDB-355503](#) and [VDB-355504](#).

## 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: 7.3

VuIDB Meta Temp Score: 6.6

VuIDB Base Score: 7.3

VuIDB Temp Score: 6.6

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

04/06/2026		Advisory disclosed
04/06/2026	+0 days	VulDB entry created
04/06/2026	+0 days	VulDB entry last update

## Sources

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

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

**Status:** Not defined

**CVE:** [CVE-2026-5689](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-5689](#)

**GCVE (VulDB):** [GCVE-100-355516](#)

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

**See also:** 🔒

## Entry

**Created:** 04/06/2026 12:32 PM

**Changes:** 04/06/2026 12:32 PM (56)

**Complete:** 🔍

**Submitter:** [LtzHust2](#)

**Cache ID:** 57:299:179

## Submit

**Accepted**

- [Submit #792946](#): Totolink A7100RU 7.4cu.2313\_b20191024 Command Injection (by LtzHust2)

## Discussion

No comments yet. Languages: en.

Please log in to comment.