



VDB-356379 · CVE-2026-5853 · GCVE-100-356379

TOTOLINK A7100RU 7.4CU.2313_B20191024 CGI /CGI-BIN/CSTECGI.CGI SETIPV6LANCFG ADDRPREFIXLEN OS COMMAND INJECTION

CVSS Meta Temp Score ⓘ

8.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.30-

Summary

A vulnerability identified as **critical** has been detected in [Totolink A7100RU 7.4cu.2313_b20191024](#). Affected by this issue is the function `setIpv6LanCfg` of the file `/cgi-bin/cstecgi.cgi` of the component *CGI Handler*. Performing a manipulation of the argument `addrPrefixLen` results in os command injection. This vulnerability is cataloged as [CVE-2026-5853](#). It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability was found in [Totolink A7100RU 7.4cu.2313_b20191024](#). It has been classified as **critical**. This affects the function `setIpv6LanCfg` of the file `/cgi-bin/cstecgi.cgi` of the component *CGI Handler*. The manipulation of the argument `addrPrefixLen` with an unknown input leads to a os command injection vulnerability. CWE is classifying the issue as [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. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-5853](#). The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details and a public exploit are known. The attack technique deployed by this issue is [T1202](#) according to MITRE ATT&CK.

The exploit is shared for download 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.

The entries [VDB-355506](#), [VDB-355515](#), [VDB-355516](#) and [VDB-355517](#) are related to this item.

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-2026-5853](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5853](#)

GCVE (VulDB): [GCVE-100-356379](#)

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

See also: 🔒

Entry

Created: 04/08/2026 09:25 PM

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

Complete: 🔍

Submitter: [LtzHuster2](#)

Cache ID: 20:B49:179

Submit

Accepted

- [Submit #791274](#): Totolink A7100RU 7.4cu.2313_b20191024 Command Injection (by LtzHuster2)

Discussion

No comments yet. Languages: en.

Please log in to comment.