VDB-356976 · CVE-2026-6116 · SUBMIT #356976

TOTOLINK A7100RU 7.4CU.2313_B20191024 CGI /CGI-BIN/CSTECGI.CGI SETDIAGNOSISCFG IP OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.9	$0-$5k	2.92

Summary

A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024 and classified as critical. This issue affects the function `setDiagnosisCfg` of the file */cgi-bin/cstecgi.cgi* of the component *CGI Handler*. The manipulation of the argument *ip* results in os command injection. This vulnerability is identified as CVE-2026-6116. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability classified as critical has been found in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function `setDiagnosisCfg` of the file */cgi-bin/cstecgi.cgi* of the component *CGI Handler*. The manipulation of the argument `ip` 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.

The advisory is shared for download at github.com. This vulnerability is traded as CVE-2026-6116. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1202.

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 vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-21708).

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: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/12/2026	+1 days	VulDB entry last update

Sources

Vendor: totolink.net

Advisory: github.com
Status: Not defined

CVE: CVE-2026-6116 (🔒)
GCVE (CVE): GCVE-0-2026-6116
GCVE (VulDB): GCVE-100-356976
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/11/2026 10:23 AM
Updated: 04/12/2026 10:10 AM
Changes: 04/11/2026 10:23 AM (57), 04/12/2026 10:10 AM (1)
Complete: 🔍
Submitter: LtzHust2
Cache ID: 52:846:179

Submit

Accepted

- Submit #792249: Totolink A7100RU 7.4cu.2313_b20191024 Command Injection (by LtzHust2)

Discussion

No comments yet. Languages: en.

Please log in to comment.