VDB-307372 · CVE-2025-4268 · GCVE-100-307372

TOTOLINK A720R 4.1.5CU.374 /CGI-BIN/CSTECGI.CGI TOPICURL MISSING AUTHENTICATION

A vulnerability has been found in TOTOLINK A720R 4.1.5cu.374 and classified as critical. This vulnerability affects some unknown functionality of the file */cgi-bin/cstecgi.cgi*. The manipulation of the argument `topicurl` with the input value `RebootSystem` leads to a missing authentication vulnerability. The CWE definition for the vulnerability is CWE-306. The product does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. As an impact it is known to affect availability.

The advisory is shared for download at github.com. This vulnerability was named CVE-2025-4268. 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.

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.

The entries VDB-304843, VDB-304844, VDB-304845 and VDB-304846 are pretty similar.

Product

Vendor

- TOTOLINK

Name

- A720R

Version

- 4.1.5cu.374

License

- commercial

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 5.0

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 5.3
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Missing authentication
CWE: CWE-306 / CWE-287
CAPEC: 🔒

ATT&CK: 🔒

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

05/04/2025		Advisory disclosed
05/04/2025	+0 days	VulDB entry created
05/05/2025	+1 days	VulDB entry last update

Sources

Vendor: totolink.net

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4268 (🔒)
GCVE (CVE): GCVE-0-2025-4268
GCVE (VulDB): GCVE-100-307372
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/04/2025 08:29 PM
Updated: 05/05/2025 10:19 AM
Changes: 05/04/2025 08:29 PM (56), 05/05/2025 10:19 AM (30)
Complete: 🔍
Submitter: 153528990
Cache ID: 5:AB4:101

Submit

Accepted

- Submit #563429: TOTOLINK A720R V4.1.5cu.374 Missing Authentication (by 153528990)

Discussion

No comments yet. Languages: en.

Please log in to comment.