VDB-307373 · CVE-2025-4269 · GCVE-100-307373

TOTOLINK A720R 4.1.5CU.374 LOG /CGI-BIN/CSTECGI.CGI TOPICURL ACCESS CONTROL

A vulnerability was found in TOTOLINK A720R 4.1.5cu.374 and classified as critical. This issue affects an unknown part of the file */cgi-bin/cstecgi.cgi* of the component *Log Handler*. The manipulation of the argument `topicurl` with the input value `clearDiagnosisLog/clearSyslog/clearTracerouteLog` leads to a access control vulnerability. Using CWE to declare the problem leads to CWE-284. The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor. Impacted is integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2025-4269. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1068 for this issue.

The exploit is available 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.

See VDB-304843, VDB-304844, VDB-304845 and VDB-304846 for similar entries.

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: 6.5
VulDB Meta Temp Score: 6.2

VulDB Base Score: 6.5
VulDB Temp Score: 5.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 6.5
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Access control
CWE: CWE-284 / CWE-266
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-2025-4269 (🔒)
GCVE (CVE): GCVE-0-2025-4269
GCVE (VulDB): GCVE-100-307373
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 (57), 05/05/2025 10:19 AM (30)
Complete: 🔍
Submitter: 153528990
Cache ID: 5:F83:101

Submit

Accepted

- Submit #563430: TOTOLINK A720R V4.1.5cu.374 Improper Access Controls (by 153528990)

Duplicate

- [redacted]
- [redacted]

Discussion

No comments yet. Languages: en.

Please log in to comment.