



VDB-307375 · CVE-2025-4271 · GCVE-100-307375

TOTOLINK A720R 4.1.5CU.374 /CGI-BIN/CSTECGI.CGI TOPICURL INFORMATION DISCLOSURE

A vulnerability was found in TOTOLINK A720R 4.1.5cu.374. It has been declared as problematic. Affected by this vulnerability is an unknown code block of the file `/cgi-bin/cstecgi.cgi`. The manipulation of the argument `topicurl` with the input value `showSyslog` leads to a information disclosure vulnerability. The CWE definition for the vulnerability is CWE-200. The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. As an impact it is known to affect confidentiality.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2025-4271. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1592 according to MITRE ATT&CK.

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.

Similar entries are available at VDB-304843, VDB-304844, VDB-304845 and VDB-304846.

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

CVSSv2	CVSSv3	CVSSv4	CVSSv2	CVSSv3	CVSSv4
5.3	5.3	5.3	5.3	5.3	5.3
4.8	4.8	4.8	4.8	4.8	4.8
5.0	5.0	5.0	5.0	5.0	5.0

VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Information disclosure

CWE: CWE-200 / 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-2025-4271 ()

GCVE (CVE): GCVE-0-2025-4271

GCVE (VulDB): GCVE-100-307375

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

See also: 

Entry

Created: 05/04/2025 08:30 PM

Updated: 05/05/2025 10:32 AM

Changes: 05/04/2025 08:30 PM (56), 05/05/2025 10:32 AM (30)

Complete: 🔍

Submitter: 153528990

Cache ID: 5:E5B:101

Submit

Accepted

- Submit #563444: TOTOLINK A720R V4.1.5cu.374 Exposure of Sensitive System Information to an Unauthorized Cont (by 153528990)

Discussion

No comments yet. Languages: en.

Please log in to comment.