



VDB-308079 · CVE-2025-4460 · GCVE-100-308079

# TOTOLINK N150RT 3.4.0-B20190525 URL FILTERING PAGE CROSS SITE SCRIPTING

A vulnerability classified as problematic has been found in TOTOLINK N150RT 3.4.0-B20190525. This affects some unknown functionality of the component *URL Filtering Page*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This is going to have an impact on integrity.

It is possible to read the advisory at [github.com](https://github.com). This vulnerability is uniquely identified as CVE-2025-4460. The exploitability is told to be easy. It is possible to initiate the attack remotely. Additional levels of successful authentication are needed for exploitation. It demands that the victim is doing some kind of user interaction. Technical details are unknown but a public exploit is available. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

The exploit is shared for download at [github.com](https://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-306325, VDB-306326, VDB-306327 and VDB-306328 are related to this item.

## Product

### Vendor

- TOTOLINK

### Name

- N150RT

### Version

- 3.4.0-B20190525

### 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: 2.4

VulDB Meta Temp Score: 2.3

VulDB Base Score: 2.4

VulDB Temp Score: 2.2

VulDB Vector: 

VulDB Reliability: 

CNA Base Score: 2.4

CNA Vector: 

## CVSSv2

| CVSSv2 Base Score | CVSSv2 Temp Score | CVSSv2 Base Score | CVSSv2 Temp Score | CVSSv2 Base Score | CVSSv2 Temp Score |
|-------------------|-------------------|-------------------|-------------------|-------------------|-------------------|
| 2.4               | 2.2               | 2.4               | 2.2               | 2.4               | 2.2               |
| 2.4               | 2.2               | 2.4               | 2.2               | 2.4               | 2.2               |
| 2.4               | 2.2               | 2.4               | 2.2               | 2.4               | 2.2               |

VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

## Exploiting

**Class:** Cross site scripting

**CWE:** CWE-79 / CWE-94 / CWE-74

**CAPEC:** 

ATT&CK: 🔒

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

|            |         |                         |
|------------|---------|-------------------------|
| 05/08/2025 |         | Advisory disclosed      |
| 05/08/2025 | +0 days | VulDB entry created     |
| 05/09/2025 | +1 days | VulDB entry last update |

## Sources

Vendor: totolink.net

Advisory: github.com  
Status: Not defined

CVE: CVE-2025-4460 (🔒)  
GCVE (CVE): GCVE-0-2025-4460

**GCVE (VulDB):** GCVE-100-308079

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

**See also:** 

## Entry

**Created:** 05/08/2025 09:12 PM

**Updated:** 05/09/2025 02:00 PM

**Changes:** 05/08/2025 09:12 PM (54), 05/09/2025 02:00 PM (30)

**Complete:** 

**Submitter:** lcyf-fizz

**Cache ID:** 5:CE3:101

## Submit

### Accepted

- Submit #565956: TOTOLINK N150RT V3.4.0-B20190525 Cross Site Scripting (by lcyf-fizz)

## Discussion

No comments yet. Languages: en.

Please log in to comment.