



VDB-308081 · CVE-2025-4462 · GCVE-100-308081

TOTOLINK N150RT 3.4.0-B20190525 /BOAFRM/FORMWSC LOCALPIN BUFFER OVERFLOW

A vulnerability, which was classified as critical, has been found in TOTOLINK N150RT 3.4.0-B20190525. This issue affects an unknown code of the file `/boafrm/formWsc`. The manipulation of the argument `localPin` with an unknown input leads to a buffer overflow vulnerability. Using CWE to declare the problem leads to CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2025-4462. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known.

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.

Entries connected to this vulnerability are available at VDB-306323 and VDB-306329.

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: 8.8

VulDB Meta Temp Score: 8.4

VulDB Base Score: 8.8

VulDB Temp Score: 8.0

VulDB Vector: 

VulDB Reliability: 

CNA Base Score: 8.8

CNA Vector: 

CVSSv2

VulDB		CNA		CVSSv2	
Base Score	Temp Score	Base Score	Temp Score	Base Score	Temp Score
8.8	8.0	8.8	8.4	8.8	8.0
8.8	8.0	8.8	8.4	8.8	8.0
8.8	8.0	8.8	8.4	8.8	8.0

VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Buffer overflow

CWE: CWE-120 / CWE-119

CAPEC: 

ATT&CK: 

Local: No

Remote: Yes

Entry

Created: 05/08/2025 09:12 PM

Updated: 05/09/2025 02:00 PM

Changes: 05/08/2025 09:12 PM (55), 05/09/2025 02:00 PM (30)

Complete: 🔍

Submitter: lcyf-fizz

Cache ID: 5:C56:101

Submit

Accepted

- Submit #565958: TOTOLINK N150RT V3.4.0-B20190525 Buffer Overflow (by lcyf-fizz)

Discussion

No comments yet. Languages: en.

Please log in to comment.