



VDB-350408 · CVE-2026-3973 · GCVE-100-350408

TENDA W3 1.0.0.3(2204) POST PARAMETER /GOFORM/SETAUTOPING FORMSETAUTOPING PING1/PING2 STACK-BASED OVERFLOW

CVSS Meta Temp Score 

8.4

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

0.34

Summary

A vulnerability, which was classified as **critical**, was found in **Tenda W3 1.0.0.3(2204)**. This vulnerability affects the function `formSetAutoPing` of the file `/goform/setAutoPing` of the component *POST Parameter Handler*. Such manipulation of the argument `ping1/ping2` leads to stack-based overflow. This vulnerability is listed as **CVE-2026-3973**. The attack may be performed from remote. In addition, an exploit is available.

Details

A vulnerability, which was classified as **critical**, has been found in **Tenda W3 1.0.0.3(2204)**. Affected by this issue is the function `formSetAutoPing` of the file `/goform/setAutoPing` of the component *POST Parameter Handler*. The manipulation of the argument `ping1/ping2` with an unknown input leads to a stack-based overflow vulnerability. Using CWE to declare the problem leads to **CWE-121**. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). Impacted is confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is handled as **CVE-2026-3973**. The exploitation is known to be easy. The attack may be launched 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.

See [VDB-206268](#), [VDB-209508](#), [VDB-214706](#) and [VDB-215149](#) for similar entries.

Product

Type

- Router Operating System

Vendor

- Tenda

Name

- W3

Version

- 1.0.0.3(2204)

License

- commercial

Website

- Vendor: <https://www.tenda.com.cn/>

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

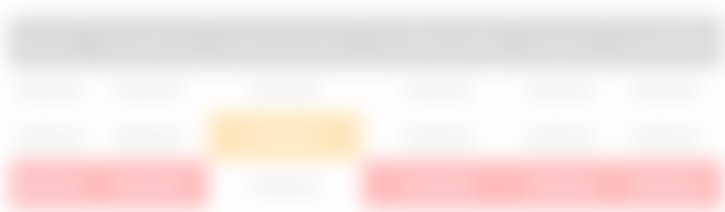
VulDB Vector: 🔒

VulDB Reliability: 🔍

CNA Base Score: 8.8

CNA Vector: 🔒

CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Stack-based overflow

CWE: [CWE-121](#) / [CWE-119](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

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

- 03/11/2026 | Advisory disclosed
- 03/11/2026 | +0 days | VulDB entry created
- 03/17/2026 | +6 days | VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-3973](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-3973](#)

GCVE (VulDB): [GCVE-100-350408](#)

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

See also: 🗝️

Entry

Created: 03/11/2026 03:06 PM

Updated: 03/17/2026 06:56 AM

Changes: 03/11/2026 03:06 PM (56), 03/11/2026 03:07 PM (2), 03/17/2026 06:56 AM (32)

Complete: 🔍

Submitter: [Svigo_o](#)

Cache ID: 20:B64:179

Submit

Accepted

- [Submit #769173](#): Tenda W3 V1.0.0.3(2204) Buffer Overflow (by Svigo_o)

Duplicate

- [\[blurred\]](#)
- [\[blurred\]](#)
- [\[blurred\]](#)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)