



VDB-349766 · CVE-2026-3799 · EUVD-2026-10293

TENDA I3 1.0.0.6(2204) /GIFORM/SETCFM FORMSETCFM FUNCpara1 STACK-BASED OVERFLOW

Summary

A vulnerability was found in [Tenda i3 1.0.0.6\(2204\)](#) and classified as **critical**. Affected is the function `formSetCfm` of the file `/goform/setcfm`. Such manipulation of the argument `funcpara1` leads to stack-based overflow. This vulnerability is documented as [CVE-2026-3799](#). The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability was found in [Tenda i3 1.0.0.6\(2204\)](#). It has been rated as **critical**. Affected by this issue is the function `formSetCfm` of the file `/goform/setcfm`. The manipulation of the argument `funcpara1` 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 available at [github.com](#). This vulnerability is handled as [CVE-2026-3799](#). 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.

The vulnerability is also documented in the vulnerability database at EUVD ([EUVD-2026-10293](#)).

Product

Type

- [Router Operating System](#)

Vendor

- [Tenda](#)

Name

- i3

Version

- 1.0.0.6(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

03/08/2026		Advisory disclosed
03/08/2026	+0 days	VulDB entry created
03/09/2026	+1 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-3799](#) 🗝️

GCVE (CVE): [GCVE-0-2026-3799](#)

GCVE (VulDB): [GCVE-100-349766](#)

EUVD: 🗝️

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

Entry

Created: 03/08/2026 01:39 PM

Updated: 03/09/2026 11:59 AM

Changes: 03/08/2026 01:39 PM (57), 03/09/2026 08:14 AM (31), 03/09/2026 11:59 AM (1)

Complete: 🔍

Submitter: [Svigo](#)

Cache ID: 68:73B:179

Submit

Accepted

- [Submit #768976](#): Tenda i3 V1.0.0.6(2204) Buffer Overflow (by Svigo)

Duplicate

-

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)