



VDB-348263 · CVE-2026-3378 · EUVD-2026-9114

TENDA F453 1.0.0.3 /GOFORM/QOSSETTING FROMQOSSETTING QOS BUFFER OVERFLOW

CVSS Meta Temp Score

8.4

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

0.20

Summary

A vulnerability classified as **critical** has been found in **Tenda F453 1.0.0.3**. This vulnerability affects the function `fromqossetting` of the file `/goform/qossetting`. The manipulation of the argument `qos` leads to buffer overflow. This vulnerability is listed as **CVE-2026-3378**. The attack may be initiated remotely. In addition, an exploit is available.

Details

A vulnerability was found in **Tenda F453 1.0.0.3**. It has been rated as **critical**. This issue affects the function `fromqossetting` of the file `/goform/qossetting`. The manipulation of the argument `qos` 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.

It is possible to read the advisory at github.com. The identification of this vulnerability is **CVE-2026-3378**. 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.

The vulnerability is also documented in the databases at CNNVD (**CNNVD-202603-019**) and EUVD (**EUVD-2026-9114**). See **VDB-260911**, **VDB-261333**, **VDB-273984** and **VDB-274773** for similar entries.

Product

Type

- Router Operating System

Vendor

- [Tenda](#)

Name

- [F453](#)

Version

- [1.0.0.3](#)

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: Buffer overflow

CWE: [CWE-120](#) / [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

02/28/2026		Advisory disclosed
02/28/2026	+0 days	VulDB entry created
03/02/2026	+2 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-3378](https://cve.mitre.org/cve/2026/3378) (🗝️)

GCVE (CVE): [GCVE-0-2026-3378](https://www.gdsc.com.cn/gcve/0-2026-3378)

GCVE (VulDB): [GCVE-100-348263](https://www.gdsc.com.cn/gcve/100-348263)

EUVD: 🗝️

CNNVD: [CNNVD-202603-019](https://www.cnnvd.org.cn/patch/CNNVD-202603-019) - Tenda F453 安全漏洞

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

See also: 🗝️

Entry

Created: 02/28/2026 08:00 AM

Updated: 03/02/2026 05:13 PM

Changes: 02/28/2026 08:00 AM (57), 03/01/2026 05:57 AM (1), 03/01/2026 07:27 PM (31), 03/02/2026 03:56 PM (1), 03/02/2026 05:13 PM (6)

Complete: 🔍

Submitter: [LtzHust2](#)

Cache ID: 4:214:179

Submit

Accepted

- [Submit #759625](#): Tenda F453 v1.0.0.3 Buffer Access Using Size of Source Buffer (by LtzHust2)

Duplicate

- [\[REDACTED\]](#)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)