VDB-356297 · CVE-2026-5841 · GCVE-100-356297

TENDA I3 1.0.0.6(2204) HTTP R7WEBSSECURITYHANDLER PATH TRAVERSAL

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	1.73-

Summary

A vulnerability marked as critical has been reported in Tenda i3 1.0.0.6(2204). The impacted element is the function `R7WebsSecurityHandler` of the component *HTTP Handler*. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2026-5841. The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability was found in Tenda i3 1.0.0.6(2204) and classified as critical. This issue affects the function `R7WebsSecurityHandler` of the component *HTTP Handler*. The manipulation with an unknown input leads to a path traversal vulnerability. Using CWE to declare the problem leads to CWE-22. The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5841. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1006 for this issue.

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.

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: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Path traversal
CWE: CWE-22
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

Sources

Vendor: tenda.com.cn

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5841 (🔒)
GCVE (CVE): GCVE-0-2026-5841
GCVE (VulDB): GCVE-100-356297
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/08/2026 07:40 PM
Changes: 04/08/2026 07:40 PM (56)
Complete: 🔍
Submitter: Fan95
Cache ID: 20:747:179

Submit

Accepted

- Submit #789935: Tenda i3 V1.0.0.6(2204) Authentication Bypass Issues (by Fan95)

Discussion

No comments yet. Languages: en.

Please log in to comment.