



Tenda i3 HTTP R7WebsSecurityHandler path traversal

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-5841
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 05:16:06 UTC
Updated	2026-04-13 15:02:47 UTC
Description	A weakness has been identified in Tenda i3 1.0.0.6(2204). The affected element is the function R7WebsSecurityHandler of

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000820000 probability, percentile 0.240050000 (date 2026-04-15)

Problem Types: CWE-22 | CWE-22 Path Traversal

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

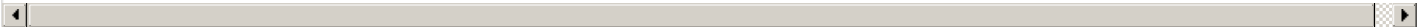
Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Tenda	I3	affected 1.0.0.6(2204)	Not specified

References				
Reference	Source	Link	Tags	
www.tenda.com.cn	cna@vuldb.com	www.tenda.com.cn		
github.com/MrXiaoFan/TendaVul/tree/main/tenda-i3-V1.0.0.6(2204)-R7WebsSe...	cna@vuldb.com	github.com		
vuldb.com/vuln/356297/cti	cna@vuldb.com	vuldb.com		
vuldb.com/submit/789935	cna@vuldb.com	vuldb.com		
vuldb.com/vuln/356297	cna@vuldb.com	vuldb.com		
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis	



Vendor Comments And Credit	
Discovery Credit	
CNA: Fan95 (VulDB User) (en)	

Additional Advisory Data		
Source	Time	Event
CNA	2026-04-08T00:00:00.000Z	Advisory disclosed
CNA	2026-04-08T02:00:00.000Z	VulDB entry created
CNA	2026-04-08T19:40:52.000Z	VulDB entry last update

CVE.report and Source URL Uptime Status status.cve.report