



CVE-2022-27022

Published on: Not Yet Published

Last Modified on: 04/14/2022 08:41:00 PM UTC

CVE-2022-27022

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ac9](#) from [Tenda](#) contain the following vulnerability:

There is a stack overflow vulnerability in the SetSysTimeCfg() function in the httpd service of Tenda AC9 V15.03.2.21_cn. The attacker can obtain a stable root shell through a constructed payload.

CVE-2022-27022 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IOT_vuln/Tenda/AC9/14 at main · EPhaha/IOT_vuln · GitHub	github.com text/html	MISC github.com/EPhaha/IOT_vuln/tree/main/Tenda/AC9/14

By selecting these links, you may be leaving CVEreport workspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Tenda	Ac9	-	All	All	All
Operating System	Tenda	Ac9 Firmware	15.03.2.21_cn	All	All	All
cpe:2.3:h:tenda:ac9:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:tenda:ac9_firmware:15.03.2.21_cn:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-27022 : There is a stack overflow vulnerability in the SetSysTimeCfg function in the httpd service of Te... twitter.com/i/web/status/1...	2022-04-07 16:07:13
 /r/netcve	CVE-2022-27022	2022-04-07 16:38:40

[← Previous ID](#)

[Next ID →](#)