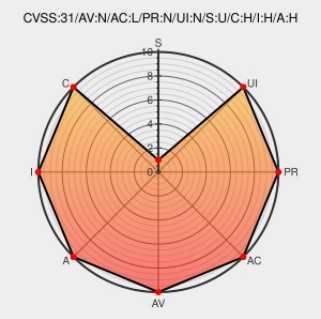
CVE-2021-46394

Published on: Not Yet Published

Last Modified on: 03/10/2022 02:41:00 PM UTC

CVE-2021-46394

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ax3 from Tenda contain the following vulnerability:

There is a stack buffer overflow vulnerability in the formSetPPTPServer function of Tenda-AX3 router V16.03.12.10_CN. The v13 variable is directly retrieved from the http request parameter startIp. Then v13 will be splice to stack by function sscanf without any security check, which causes stack overflow. By POSTing the page /goform/SetPptpServerCfg with proper startIp, the attacker can easily perform remote code execution with carefully crafted overflow data.

CVE-2021-46394 has been assigned by 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: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IoT-CVE/Tenda/AX3/4 at main · sec-bin/IoT-CVE · GitHub	github.com text/html	MISC github.com/sec-bin/IoT-CVE/tree/main/Tenda/AX3/4

By selecting these links, you may be leaving CVEreport webspace. 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	Ax3	-	All	All	All
Operating System	Tenda	Ax3 Firmware	16.03.12.10	All	All	All

cpe:2.3:h:tenda:ax3:-:*:*:*:*:*:*:*:

cpe:2.3:o:tenda:ax3_firmware:16.03.12.10:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-46394 : There is a stack buffer overflow vulnerability in the formSetPPTPServer function of Tenda-AX3 rout… twitter.com/i/web/status/1…	2022-03-04 14:05:00
/r/netcve	CVE-2021-46394	2022-03-04 15:38:33

← Previous ID

Next ID→