



CVE-2017-16923

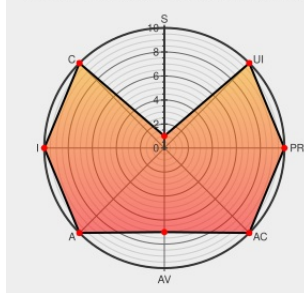
Published on: 11/21/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-16923

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

CVSS:30/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Ac15](#) from [Tenda](#) contain the following vulnerability:

Command Injection vulnerability in app_data_center on Shenzhen Tenda Ac9 US_AC9V1.0BR_V15.03.05.14_multi_TD01, Ac9 ac9_kf_V15.03.05.19(6318_)_cn, Ac15 US_AC15V1.0BR_V15.03.05.18_multi_TD01, Ac15 US_AC15V1.0BR_V15.03.05.19_multi_TD01, Ac18 US_AC18V1.0BR_V15.03.05.05_multi_TD01, and Ac18

ac18_kf_V15.03.05.19(6318_)_cn devices allows remote unauthenticated attackers to execute arbitrary OS commands via a crafted cgi-bin/luci/usbeject?dev_name= GET request from the LAN. This occurs because the "sub_A6E8 usbeject_process_entry" function executes a system function with untrusted input.

CVE-2017-16923 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **8.3 - HIGH**

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

CVE References

Description	Tags	Link				
Poc/Router/Tenda at master · lolop/Poc · GitHub	Issue Tracking Third Party Advisory github.com text/html	 MISC github.com/lolop/Poc/tree/master/Router/Tenda				
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	Ac15	-	All	All	All
Hardware 	Tenda	Ac15	-	All	All	All
Operating System	Tenda	Ac15 Firmware	us_ac15v1.0br_v15.03.05.18_multi_td01	All	All	All
Operating System	Tenda	Ac15 Firmware	us_ac15v1.0br_v15.03.05.19_multi_td01	All	All	All
Operating System	Tenda	Ac15 Firmware	us_ac15v1.0br_v15.03.05.18_multi_td01	All	All	All
Operating System	Tenda	Ac15 Firmware	us_ac15v1.0br_v15.03.05.19_multi_td01	All	All	All
Hardware 	Tenda	Ac18	-	All	All	All
Hardware 	Tenda	Ac18	-	All	All	All
Operating System	Tenda	Ac18 Firmware	ac18_kf_v15.03.05.19(6318_)_cn	All	All	All
Operating System	Tenda	Ac18 Firmware	ac18_kf_v15.03.05.19(6318_)_cn	All	All	All
Operating System	Tenda	Ac18 Firmware	us_ac18v1.0br_v15.03.05.05_multi_td01	All	All	All
Operating System	Tenda	Ac18 Firmware	ac18_kf_v15.03.05.19(6318_)_cn	All	All	All
Operating System	Tenda	Ac18 Firmware	us_ac18v1.0br_v15.03.05.05_multi_td01	All	All	All
Hardware 	Tenda	Ac9	-	All	All	All
Hardware 	Tenda	Ac9	-	All	All	All
Operating System	Tenda	Ac9 Firmware	ac9_kf_v15.03.05.19(6318_)_cn	All	All	All
Operating System	Tenda	Ac9 Firmware	ac9_kf_v15.03.05.19(6318_)_cn	All	All	All

← Previous ID

Next ID →

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)