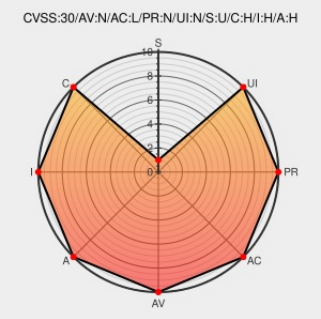
CVE-2017-11519

Published on: 07/21/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

CVE-2017-11519

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



Certain versions of Archer C9 2.0 from Tp-link contain the following vulnerability:

passwd_recovery.lua on the TP-Link Archer C9(UN)_V2_160517 allows an attacker to reset the admin password by leveraging a predictable random number generator seed. This is fixed in C9(UN)_V2_170511.

CVE-2017-11519 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: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Download for Archer C9 V2 - Welcome to TP-LINK	Third Party Advisory, www.tp-link.com, text/html	MISC www.tp-link.com/en/download/Archer-C9_V2.html#Firmware
TP-Link Archer C9 - Admin Password Reset and RCE (CVE-	Exploit	MISC devcraft.io/posts/2017/07/21/tp-link-archer-

2017-11519) | devcraft.io

Third Party Advisory
devcraft.io
text/html
c9-admin-password-reset.html

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

Exploit/POC from Github

POC for TP-Link Archer C9 - Admin Password Reset and RCE (CVE-2017-11519)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer C9 2.0	-	All	All	All
Operating System	Tp-link	Archer C9 2.0 Firmware	160517	All	All	All
Hardware	Tp-link	Archer C9 2.0	-	All	All	All
Hardware	Tp-link	Archer C9 2.0	-	All	All	All
Operating System	Tp-link	Archer C9 2.0 Firmware	160517	All	All	All
Operating System	Tp-link	Archer C9 2.0 Firmware	160517	All	All	All

cpe:2.3:h:tp-link:archer_c9_(2.0):-:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:archer_c9_(2.0)_firmware:160517:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:archer_c9_\(2.0\):-:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:archer_c9_\(2.0\):-:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:archer_c9_\(2.0\)_firmware:160517:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:archer_c9_\(2.0\)_firmware:160517:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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