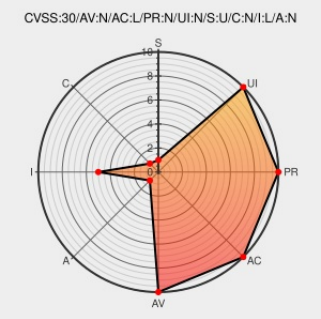
CVE-2017-8217

Published on: 04/25/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:43 PM UTC

CVE-2017-8217

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



Certain versions of C2 from Tp-link contain the following vulnerability:

TP-Link C2 and C20i devices through firmware 0.9.1 4.2 v0032.0 Build 160706 Rel.37961n have too permissive iptables rules, e.g., SNMP is not blocked on any interface.

CVE-2017-8217 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.3 - MEDIUM

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

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
TP-Link C2 and C20i vulnerable to command injection (authenticated root RCE), DoS, improper firewall rules - IT Security Research by Pierre	Exploit Technical Description Third Party Advisory pierrekim.github.io text/html	MISC pierrekim.github.io/blog/2017-02-09-tplink-c2-and-c20i-vulnerable.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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	C2	-	All	All	All
Hardware	Tp-link	C2	-	All	All	All
Hardware	Tp-link	C20i	-	All	All	All
Hardware	Tp-link	C20i	-	All	All	All
Operating System	Tp-link	C20i Firmware	All	rel.37961n	All	All
Operating System	Tp-link	C2 Firmware	All	rel.37961n	All	All

cpe:2.3:h:tp-link:c2:-:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:c2:-:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:c20i:-:*:*:*:*:*:*:*:

cpe:2.3:h:tp-link:c20i:-:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:c20i_firmware:*:rel.37961n:*:*:*:*:*:*:

cpe:2.3:o:tp-link:c2_firmware:*:rel.37961n:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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