



CVE-2020-17891

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-17891
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-14 20:15:00 UTC
Updated	2021-05-21 13:24:00 UTC
Description	TP-Link Archer C1200 firmware version 1.13 Build 2018/01/24 rel.52299 EU has a XSS vulnerability allowing a remote att

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer C1200	-	All	All	All
Operating System	Tp-link	Archer C1200 Firmware	1.13	52299	All	All

References

Reference	Source	Link	Tags
GitHub - sandboxescape/TP-Link-wireless-router-Archer-C1200---Cross-Site-Scripting	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)