



CVE-2022-41783

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

Summary

CVE	CVE-2022-41783
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-07 04:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	tdpServer of TP-Link RE300 V1 improperly processes its input, which may allow an attacker to cause a denial-of-service (D

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Re3000	1.0	All	All	All
Operating System	Tp-link	Re3000 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
Download for RE300 TP-Link	MISC	www.tp-link.com	
JVN#29657972: TP-Link RE300 V1 tdpServer vulnerable to improper processing of its input	MISC	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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