CVE-2018-18541

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-18541
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-20 22:29:00 UTC
Updated	2019-07-23 18:15:00 UTC
Description	In Teeworlds before 0.6.5, connection packets could be forged. There was no challenge-response involved in the connectio

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Teeworlds	Teeworlds	All	All	All	All
Application	Teeworlds	Teeworlds	All	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2019:1999-1: moderate: Security update f	SUSE	lists.opensuse.org	
#911487 - teeworlds: CVE-2018-18541: remote denial-of-service - Debian Bug report logs	MISC	bugs.debian.org	Mailing List, Pa
CVE: Remote denial-of-service fixed in 0.6.5 · Issue #1536 · teeworlds/teeworlds · GitHub	MISC	github.com	Patch, Vendor
Debian -- Security Information -- DSA-4329-1 teeworlds	DEBIAN	www.debian.org	Third Party Adv
Teeworlds	MISC	teeworlds.com	Vendor Adviso
[security-announce] openSUSE-SU-2019:1793-1: moderate: Security update f	SUSE	lists.opensuse.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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