CVE-2016-9400

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

Summary

CVE	CVE-2016-9400
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-22 16:59:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	The CClient::ProcessServerPacket method in engine/client/client.cpp in Teeworlds before 0.6.4 allows remote servers to wr

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Teeworlds	Teeworlds	All	All	All	All
Application	Teeworlds	Teeworlds	All	All	All	All

References

Reference	Source	Link	T
oss-security - CVE Request: teeworlds: possible remote code execution on teeworlds client	MLIST	www.openwall.com	M
added some checks to snap handling · teeworlds/teeworlds@ff25472 · GitHub	CONFIRM	github.com	I
Teeworlds 'client.cpp' Memory Corruption Vulnerability	BID	www.securityfocus.com	T
oss-security - Re: CVE Request: teeworlds: possible remote code execution on teeworlds client	MLIST	www.openwall.com	M
Teeworlds: Remote execution of arbitrary code on client (GLSA 201705-13) — Gentoo security	GENTOO	security.gentoo.org	T
[SECURITY] Fedora 23 Update: teeworlds-0.6.4-1.fc23 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	T
[SECURITY] Fedora 23 Update: teeworlds-0.6.4-1.fc23 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
Teeworlds	CONFIRM	www.teeworlds.com	V
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710489 Gentoo Linux Teeworlds Remote execution of arbitrary code on client Vulnerability (GLSA 201705-13)