



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 w

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
oss-security - CVE Request: teeworlds: possible remote code execution on teeworlds client	MLIST	www.openwall.com
added some checks to snap handling · teeworlds/teeworlds@ff25472 · GitHub	CONFIRM	github.com
Teeworlds 'client.cpp' Memory Corruption Vulnerability	BID	www.securityfocus.com
oss-security - Re: CVE Request: teeworlds: possible remote code execution on teeworlds client	MLIST	www.openwall.com
Teeworlds: Remote execution of arbitrary code on client (GLSA 201705-13) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 23 Update: teeworlds-0.6.4-1.fc23 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 23 Update: teeworlds-0.6.4-1.fc23 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Teeworlds	CONFIRM	www.teeworlds.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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)

© [CVE.report](#) 2026 |

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 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](#)