



CVE-2017-6471

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

Summary

CVE	CVE-2017-6471
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-04 03:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a WSP infinite loop, triggered by packet injection or a malformed cap

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	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-3811-1 wireshark	DEBIAN	www.debian.org	Third Party Advisory
code.wireshark Code Review - wireshark.git/commit	CONFIRM	code.wireshark.org	Issue Tracking, Patch, Vendo
Wireshark WSP Dissector 'tcp_graph.c' Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB En
Wireshark · wnpa-sec-2017-05 · WSP infinite loop	CONFIRM	www.wireshark.org	Vendor Advisory
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
13348 – Fuzzed PCAP causes large memory usage in dissect_wsp	CONFIRM	bugs.wireshark.org	Issue Tracking, Patch, Vendo
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.

Legacy QID Mappings

501299 Alpine Linux Security Update for wireshark

© [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](#)