



CVE-2019-9208

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

Summary

CVE	CVE-2019-9208
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-28 04:29:00 UTC
Updated	2023-11-07 03:13:00 UTC
Description	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the TCAP dissector could crash. This was addressed in epan/dissectors/asr

Risk And Classification

Problem Types: CWE-476

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	Wireshark	Wireshark	All	All	All	All
Application	Wireshark	Wireshark	All	All	All	All

References

Reference	Source	Link	Ta
Debian -- Security Information -- DSA-4416-1 wireshark	DEBIAN	www.debian.org	Th
Wireshark Multiple Denial of Service Vulnerabilities	BID	www.securityfocus.com	Th
[security-announce] openSUSE-SU-2019:1108-1: moderate: Security update f	SUSE	lists.opensuse.org	
Bugtraq: [SECURITY] [DSA 4416-1] wireshark security update	BUGTRAQ	seclists.org	Me
code.wireshark Code Review - wireshark.git/commit		code.wireshark.org	
Wireshark · wnpa-sec-2019-07 · TCAP dissector crash	MISC	www.wireshark.org	Ve
[security-announce] openSUSE-SU-2020:0362-1: moderate: Security update f	SUSE	lists.opensuse.org	
code.wireshark Code Review - wireshark.git/commit	MISC	code.wireshark.org	Pa
Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.com	
USN-3986-1: Wireshark vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	

[security-announce] openSUSE-SU-2019:1390-1: moderate: Security update f	SUSE	lists.opensuse.org	
15464 – Wireshark NULL pointer dereference in dissect_tcapy_application_context_name	MISC	bugs.wireshark.org	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296087](#) Oracle Solaris 11.4 Support Repository Update (SRU) 8.1.5 Missing (CPUAPR2019)

[501315](#) 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)